Relazione2018

Relazione2018

I numeri del 2018

Provvedimenti collegiali 517

130 Ricorsi decisi

159 Ordinanze-ingiunzione

37 Verifiche preliminari

28 Pareri resi al Governo

44 Pareri accesso civico

5.640 Riscontri a segnalazioni e reclami

€ 8.161.806 Sanzioni riscosse

150 Ispezioni

488 Sanzioni contestate

109 Riunioni internazionali

27 Comunicazioni all'autorità giudiziaria

22.802 Risposte a quesiti

50 Comunicati e *newsletter*

5.417.249 Accessi al sito web

Indice

Indice

I - STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

II – L'ATTIVITÀ SVOLTA DAL GARANTE

Indice

Indice

Avvertenza ed elenco delle abbreviazioni e degli acronimi più ricorrenti

La presente Relazione è riferita al 2018 e contiene talune notizie già anticipate nella precedente edizione nonché informazioni relative a sviluppi che si è ritenuto opportuno menzionare.

Arera	Autorità di regolazione per energia reti e ambiente
Aifa	Agenzia italiana del farmaco
Agcm	Autorità garante per la concorrenza e il mercato
Agcom	Autorità per le garanzie nelle comunicazioni
AgID	Agenzia per l'Italia Digitale
All.	Allegato
Anac	Autorità nazionale anticorruzione
art.	articolo
carta d'identità elettronica	Cie
c.c.	codice civile
C.d.S.	Consiglio di Stato
c.p.	codice penale
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
Cad	Codice dell'amministrazione digitale
cap.	capitolo
cd.	cosiddetto/i
cfr.	confronta
CGUE	Corte di giustizia dell'Unione europea
cit.	citato
Codice	Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101)
Comitato europeo per la protezione dei dati	CEPD
Consob	Commissione nazionale per le società e la borsa
Corte EDU	Corte europea dei diritti dell'uomo
Cost.	Costituzione
d.d.l.	disegno di legge
d.l.	decreto-legge

d.lgs.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.R.	decreto del Presidente della Repubblica
doc.	documento
es.	esempio
Fse	Fascicolo sanitario elettronico
G.U.	Gazzetta ufficiale della Repubblica italiana
GUUE	Gazzetta ufficiale dell'Unione europea
Gruppo Art. 29	Gruppo dei garanti europei istituto dall'art. 29 della direttiva 95/46/CE
IWGDPT	*International Working Group on Data Protection in Telecommunications*
l.	legge
lett.	lettera
Mef	Ministero dell'economia e delle finanze
Miur	Ministero dell'istruzione dell'università e della ricerca
n.	numero
p.	pagina
p.a.	pubblica amministrazione
par.	paragrafo
Pec	posta elettronica certificata
provv.	provvedimento del Garante
r.d.	regio decreto
reg.	regolamento
RGPD	regolamento (UE) 679/2016
Rpct	Responsabile della prevenzione della corruzione e della trasparenza
Rpd	Responsabile della protezione dei dati
Rpo	Registro pubblico delle opposizioni
Rspp	Responsabile del servizio prevenzione e protezione
sez.	sezione
Spid	Sistema pubblico dell'identità digitale
tab.	tabella
t.u.	testo unico
TFUE	Trattato sul funzionamento dell'Unione europea
Tulps	Testo unico delle leggi di pubblica sicurezza
UE	Unione europea
Url	*Uniform resource locator*
v.	vedi

Stato di attuazione del Codice in materia di protezione dei dati personali

I – Stato di attuazione del Codice in materia di protezione dei dati personali

1 Introduzione

1.1. Volendo ricorrere ad una semplificazione, può dirsi che il 25 maggio 2018 – data a partire dalla quale, come è noto, ha trovato applicazione il Regolamento generale sulla protezione dei dati (RGPD) – ha segnato uno spartiacque con riguardo alle attività complessivamente poste in essere dal Garante nel corso del 2018 (cfr. sez. IV, tab. 1).

Nella prima parte dell'anno, nel vigore della previgente cornice normativa, si sono per lo più definite una pluralità di istruttorie, riguardanti, in particolare, le attività di controllo e le verifiche preliminari (par. 10.1 e 14.6), ma pure finalizzate alla definizione dei ricorsi pendenti (cap. 19), peculiare tecnica per l'esercizio dei diritti da parte degli interessati rivelatasi particolarmente efficace, che, dopo aver accompagnato l'attività del Garante fin dalla sua istituzione, è venuta meno con il RGPD per essere riassorbita nello strumento generale del reclamo (par. 5.4.1; v. pure art. 19, comma 5, d.lgs. 10 agosto 2018, n. 101); parallelamente, l'Autorità ha accompagnato il processo legislativo di adeguamento del quadro normativo nazionale (cfr. par. 2.1).

Grossomodo nel secondo semestre, ed in particolare a far data dall'entrata in vigore della disciplina interna di adeguamento al RGPD – contenuta nel

Foreword

1.1. In a nutshell, one might argue that the 25th of May, 2018 – when the EU General Data Protection Regulation (GDPR) became applicable – marked a veritable watershed moment in terms of the activities carried out by the Italian supervisory authority in 2018 (Section IV, Table 1).

In the first part of the year, when the previous legal framework was applicable, several proceedings were finalised concerning, in particular, inspections and prior checking activities (paragraph 10.1 and paragraph 14.6); some of those proceedings allowed finalising pending complaints (Chapter 19) as regulated specifically by the national legislation. Such complaints proved to be especially effective to enforce the exercise of data subjects' rights throughout the past years of activity, and the relevant procedure was replaced by the more general 'complaint' procedure as set out in the GDPR (paragraph 5.4.1; see also Section 19(5) of legislative decree No. 101/2018). The legislative process intended to adapt the national legal system to the GDPR was monitored closely and in parallel by the Garante as well (paragraph 2.1).

In the latter part of the year, the SA focused conversely on the new legal framework, in particular following entry into force of the national legisla-

1

menzionato decreto legislativo n. 101/2018, che ha apportato significative modifiche al decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) –, le iniziative dell'Autorità, anche di natura organizzativa, si sono invece polarizzate sul rinnovato quadro normativo, sulla scia di quelle già precedentemente intraprese (cfr. Relazione 2017, p. 6 ss.).

E se, con riferimento al RGPD, può ritenersi che le innovazioni, pur rilevanti, si pongono comunque in linea di continuità con la disciplina previgente (essa pure di derivazione comunitaria, segnatamente dalla direttiva 95/46/CE), non possono sottacersi alcune novità: anzitutto la rafforzata cooperazione con le altre autorità di controllo (compendiate nel Capo VII del RGPD: cfr. par. 22.1); la modificata cornice normativa dedicata ai trattamenti effettuati per fini di polizia e di giustizia penale che, espunti dal Codice, trovano ora autonoma regolamentazione nel decreto legislativo 18 maggio 2018, n. 51, con il quale si è recepita la direttiva 2016/680 (par. 2.2); i vari istituti – quali la valutazione d'impatto *privacy*, la figura del responsabile per la protezione dei dati, i meccanismi di certificazione – introdotti all'insegna di una più accentuata responsabilizzazione di chi opera (anzitutto) in qualità di titolare del trattamento, essendo chiamato a rendere conto delle misure tecnico-organizzative poste in essere per assicurare la liceità dei trattamenti e il rispetto dei diritti fondamentali degli interessati (cd. *accountability*), cui fa da contrappeso un più severo quadro sanzionatorio (cfr. par. 21.7).

Quasi a voler aggiungere un elemento di complessità nella gestione della fase di transizione che il Garante è stato chiamato a governare, un cenno va alle innovazioni di natura logistica che hanno interessato l'Autorità, la quale ha trasferito a fine 2018 la propria sede in piazza Venezia (cfr. par. 26.2).

1.2. Anche sul piano sovranazionale il 2018 ha segnato un momento di pas-

tion enacted further to the GDPR – namely, legislative decree No. 101/2018 as mentioned above, which made substantial amendments to the so-called consolidated data protection code, i.e., legislative decree No. 196/2003. To a great extent, the work done was modelled after the one that had started in 2017 (see the 2017 Annual Report, p. 6 and ff.).

Whilst it could be argued that the main innovations brought about by the GDPR are, albeit substantial, in line with the preceding legislation – which was also grounded in EU law, i.e. in directive 95/46/EC – one cannot but highlight certain key changes. These include, first and foremost, the enhanced cooperation with the other EU supervisory authorities as laid down in Chapter VII of the GDPR – see paragraph 22.1; the amended rules applying to processing activities in the law enforcement sector, which have been taken out of the data protection Code as they are now regulated separately by legislative decree No. 51 of 18 May 2018 – transposing directive 2016/680 (paragraph 2.2.); the various tools – such as the data protection impact assessment, the appointment of a data protection officer, the implementation of certification mechanisms – introduced by the GDPR under the umbrella of the enhanced accountability all data controllers are expected to ensure, in that they are called upon to account for the technical and organisational measures they have put in place to achieve lawful processing activities along with respect for data subjects' fundamental rights; and the more effective sanctions envisaged against this background (see paragraph 21.7).

The complex management of this transition phase was actually compounded for the Italian SA by the new logistics arrangements following the move to its new offices in Piazza Venezia, in Rome, which took place at the end of 2018 (see paragraph 26.2).

1.2. The past year marked a transi-

saggio (cfr., nel dettaglio, cap. 22). Nell'ambito del Consiglio d'Europa si è infatti concluso il processo di modernizzazione della Convenzione 108, con l'adozione, in data 18 maggio 2018, del Protocollo emendativo della stessa (che l'Italia ha sottoscritto il 5 marzo 2019). Nell'ambito dell'Unione europea, il Comitato europeo per la protezione dei dati ha sostituito il Gruppo Art. 29 senza soluzione di continuità (nonostante le modifiche organizzative intervenute alla luce delle diversità tra i due soggetti, atteso che il nuovo Comitato è dotato di personalità giuridica e di proprio segretariato) e ha continuato a lavorare al fine di fornire indicazioni in ordine all'applicazione del nuovo quadro giuridico creato dal RGPD. In quest'ottica il Comitato ha fatto proprie le linee guida adottate in materia, a partire dal 2017, dal Gruppo Art. 29 e ha avviato numerose consultazioni pubbliche per acquisire valutazioni e commenti rispetto ai documenti adottati, specie su temi nuovi quali certificazioni, valutazione di impatto sulla protezione dei dati, notifica delle violazioni di dati personali.

A partire dal 25 maggio 2018 le autorità di protezione dei dati hanno anche dato avvio alla menzionata attività di cooperazione prevista dal RGPD al fine di prendere in esame reclami e violazioni relativi a trattamenti transfrontalieri: una rivoluzione questa che vede le autorità competenti di diversi Paesi membri decidere insieme, anche avvalendosi di una piattaforma condivisa (il Sistema di informazione del mercato interno – IMI, cfr. par. 14.8), i casi aventi impatto sovranazionale (vuoi perché il titolare effettua il trattamento in stabilimenti in diversi Paesi UE o perché ci sono soggetti interessati dal trattamento in più Paesi UE) dopo essersi scambiate le informazioni necessarie e aver portato a termine, se del caso anche congiuntamente, verifiche ispettive.

1.3. Considerando più dappresso le attività svolte dall'Autorità e collocandosi nella prospettiva della successione

tion phase at supranational level as well (see Chapter 22). The modernization process concerning Council of Europe's Convention 108/81 was also completed, so that the Amending Protocol to that Convention could be adopted on 18 May 2018; Italy signed the said Protocol on 5 March 2019. At EU level, the European Data Protection Board replaced the 'Article 29' Working Party seamlessly, even though organisational changes were made necessary on account of the different features of the Board - which has legal personality and is equipped with a Secretariat of its own. The new Board went on working to provide guidance on the implementation of the new legal framework grounded in the GDPR. In that respect, the Board endorsed the guidelines the 'Article 29' Working Party had been issuing on GDPR-related topics ever since 2017, whilst several public consultations were launched to gather inputs and suggestions on the adopted documents – with particular regard to new issues such as certifications, data protection impact assessments, and personal data breach notifications.

As from 25 May 2018, the EU SAs also started cooperating under the terms of the GDPR to handle complaints and breaches related to cross-border processing activities. This is a revolutionary approach whereby the competent authorities from several Member States are called upon to jointly decide the cases having cross-border impact, also with the help of a shared IT platform (the so-called Internal Market Information System, IMI: see paragraph 14.8). To that end, they are expected to first exchange all the necessary information and carry out inspections, where appropriate also jointly.

1.3. Coming more specifically to the activities carried out by the Italian SA and following the above time sequence, one should point out that the first six months of the past year allowed significant decisions to be made with regard to

1

cronologica cui si è fatto riferimento, nel primo semestre si registrano decisioni significative con riguardo ai compiti di controllo. Talune in settori già oggetto di intervento in passato: con particolare riguardo agli operatori di telecomunicazione, in larga misura in relazione alle violazioni poste in essere nell'ambito dei trattamenti effettuati per finalità di telemarketing, sono stati adottati provvedimenti che hanno riguardato una platea amplissima (costituita da milioni) di interessati (cfr. par. 10.2) e, conseguentemente, irrogate sanzioni per un importo complessivamente pari a € 3.440.000, di cui sono stati versati nel 2018 € 2.280.000 (e residui €600.000 nel 2019), rispetto al complessivo ammontare di € 8.161.806 riscossi dall'Autorità nel 2018 (cfr. par. 21.6.2). Altre hanno interessato ambiti finora meno esplorati, ma che assumeranno rilevanza centrale nella nuova cornice normativa, coinvolgendo attori di primario rilievo nel panorama globale. Si pensi al provvedimento adottato, all'esito della collaborazione instaurata con alcune autorità europee di protezione dei dati, in relazione ad una violazione di dati personali (*data breach*) – verificatasi nel 2016, ma resa pubblica soltanto nel novembre 2017 – che, a seguito di un attacco *hacker*, ha coinvolto su scala globale i dati di decine di milioni di utenti di un gruppo multinazionale gestore di una nota piattaforma *online* tramite la quale viene fornito un servizio di trasporto privato con l'ausilio di un'applicazione mobile volta a mettere in collegamento diretto passeggeri e autisti (par. 15.1). E, ancora, il Garante si è pronunciato in relazione alla comunicazione di dati, ritenendola illecita, tra un popolare servizio di messaggeria elettronica e la principale piattaforma globale di *social network* (par. 11.1).

Rispetto ad altri ambiti d'azione dell'Autorità si è registrato un incremento delle richieste di verifica preliminare (complessivamente 37 nel solo primo semestre 2018 rispetto alle 26 registrate nell'intero 2017), strumento previsto dall'art. 17, d.lgs. n. 196/2003,

the oversight tasks committed to the SA. Those decisions concerned, in part, sectors that had already been impacted by the SA with particular regard to telecom operators. In the latter sector, the decisions made by the SA concerned a substantial number of data subjects (up to several millions) mostly on account of breaches committed in connection with telemarketing-related processing activities (see paragraph 10.2). Accordingly, fines amounting to Euro 3,440,000 were imposed, of which Euro 2,280,000 could be levied in 2018 and the remainder was carried over to 2019 – out of a total of Euro 8,161,806 levied by the SA in 2018 (see paragraph 21.6.2). Other decisions concerned sectors that had been investigated to a lesser extent up to the past year, even though they are bound to take on a key role in the new legal framework as they involve major global players. Reference should be made in that regard to the decision that was adopted by the SA following the cooperative inquiries carried out with other EU SAs into a data breach that had taken place in 2016, but had been disclosed only in November 2017. The data breach had been caused by a hacking attack that had affected the data of tens of millions of customers worldwide of a multinational group; this group handles a well-known online platform that is intended to provide private transportation services via a mobile app connecting passengers and drivers directly (paragraph 15.1). In yet another case, the SA found that a well-known messaging service had unlawfully disclosed user data to the leading social networking platform (paragraph 11.1).

Regarding other areas of the SA's activity, prior checking requests rose to 37 in the first six months of 2018, compared to 26 throughout 2017; prior checking was regulated by Section 17 of legislative decree No. 196/2003 and several controllers relied on this tool which is no longer applicable following entry into force of the GDPR – indeed, it is now superseded by the data protec-

divenuto ormai familiare nella prassi e anch'esso venuto meno con il RGPD, per essere sostituito, nella nuova cornice normativa, dalla valutazione d'impatto *privacy*, ora prevista dall'art. 35 RGPD (v. già, in tal senso, le indicazioni dell'Autorità in relazione al prospettato monitoraggio degli automezzi adibiti al trasporto di utenti diversamente abili nonché degli spostamenti individuali dei medesimi: cfr. par. 5.4.2 e 13.2). Al di là dei settori già presi in considerazione in passato (cfr. par. 10.1, con riguardo a trattamenti effettuati per finalità di marketing e profilazione in relazione all'acquisto di beni semi-durevoli), le menzionate verifiche hanno messo in luce trattamenti sempre più sofisticati – ad esempio effettuati mediante sistemi di ripresa delle immagini "indossabili" (par. 13.4) o di videosorveglianza cd. intelligente (par. 14.4), anche in vista di una più accentuata automazione dell'esazione dei pedaggi autostradali (par. 14.5) – o imperniati su un utilizzo crescente di dati biometrici, anche da parte delle Forze di polizia (par. 7.2). Sempre più frequentemente la valutazione del Garante si è soffermata sulla localizzabilità delle persone per il tramite di appositi sensori ad esse (direttamente o indirettamente) ricollegabili. Rispetto a tali fattispecie il Garante (pur rilevando in linea di massima la liceità dei trattamenti effettuati) ha dettato misure a tutela dei diritti e della dignità degli interessati, siano essi pazienti non auto-sufficienti (dotati di un bracciale o di una cavigliera con localizzatore) (par. 5.1), ovvero, come sempre più di frequente accade, lavoratori, la cui attività è indirettamente (minutamente) monitorata per il tramite delle dotazioni di servizio (siano essi veicoli, *smartphone*, *tablet*, etc.), operanti in ambito privato (par. 13.3) o pubblico (par. 13.7 e 13.9).

1.4. Il secondo semestre è stato contrassegnato (in particolare) dall'infittirsi delle azioni volte ad allineare l'operatività dell'Autorità rispetto alla modificata cornice normativa.

Si è anzitutto realizzata un'attenta

tion impact assessment as provided for in Article 35 of the GDPR. The latter circumstance had been pointed out by the SA in connection with a prior checking request concerning the proposed surveillance of vehicles intended for the transportation of disabled individuals as well as of the individuals themselves – see paragraphs 5.4.2 and 13.2. On top of the sectors considered in the past years – see paragraph 10.1 on processing activities carried out for marketing and profiling purposes in connection with purchasing semi-durable goods – those prior checking activities allowed addressing increasingly sophisticated types of processing: from 'wearable' image recording systems (paragraph 13.4) to smart video surveillance (paragraph 14.4), partly with a view to the enhanced automation of highway toll payments (paragraph 14.5), up to the growing use of biometrics also by the police (paragraph 7.2). The SA's assessment focused increasingly on the localization of individuals by way of ad-hoc sensors that could be traced back to those individuals, whether directly or not. The SA found that the processing activities in question were lawful, in principle, but set forth measures to protect the rights and dignity of the individuals concerned – including non-autonomous patients wearing localization bracelets or anklets (paragraph 5.1) or employees, whose activities can be indirectly (and pervasively) monitored by way of the devices committed to them (vehicles, smartphones, tablets, etc.) in both the private (paragraph 13.3) and the public (paragraphs 13.7 and 13.9) sector.

1.4. The latter part of the year featured, in particular, increased work to bring the SA's operational mechanisms fully in line with the new legal framework.

The so-called 'general authorisations' applying to the processing of 'sensitive' data were revised pursuant to Section 21 of legislative decree No. 101/18, so that the provisions contained in those autho-

attività di revisione delle autorizzazioni generali (richiesta dall'art. 21, d.lgs. n. 101/2018), volta ad individuare con il provvedimento del 13 dicembre 2018, n. 497 (doc. web n. 9068972, posto in consultazione pubblica con avviso in G.U. 11 gennaio 2019, n. 9) le prescrizioni, in esse già contenute compatibili con le disposizioni del RGPD (cfr. par. 5.4.4). Con propri provvedimenti il Garante ha quindi verificato, in attuazione dell'art. 20, commi 3 e 4, d.lgs. n. 101/2018, la conformità al RGPD delle disposizioni dei codici di deontologia e di buona condotta contenuti negli Allegati A.2, A.3 e A.4 del Codice, riformulandole in "regole deontologiche" allegate al Codice (All. A) (par. 5.4.4); analogo processo ha interessato il "Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica", con l'adozione delle "Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica" (cap. 8). Anche il più articolato processo volto a salvaguardare la valenza dei codici di deontologia e di buona condotta di cui agli Allegati A.5 e A.7 del Codice è stato avviato, in conformità a quanto previsto dall'art. 20, comma 1, d.lgs. n. 101/2018 (par. 14.3).

Si è altresì provveduto ad individuare un elenco (non esaustivo) di trattamenti transfrontalieri da sottoporre a valutazione di impatto (cfr. provv. 11 ottobre 2018, n. 467, doc. web n. 9058979), ferme restando le indicazioni del Gruppo Art. 29 del 4 aprile 2017 contenute nelle "Linee guida in materia di valutazione d'impatto", da ultimo aggiornate il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (WP 248, rev. 01).

Nel solco delle iniziative già intraprese nel 2017 (cfr. Relazione 2017, p. 7 ss.), sono stati forniti ulteriori chiarimenti in relazione alla figura e al *modus operandi* dei Responsabili della protezione dei dati (Rpd), anche attraverso una serie di incontri dedicati sia al settore pubblico (cfr. par. 5.4.3) che a

risations that were compatible with the GDPR could be identified by a decision dated 13 December 2018 – on which a public consultation was launched on 11 January 2019 via a notice published in Italy's official journal (see paragraph 5.4.4). Under the terms of Section 20(3) and (4) of the said legislative decree No. 101/2018, the SA assessed to what extent the provisions set out in some of the 'Codes of practice and conduct' attached to the data protection Code were compatible with the GDPR (in particular, the codes contained in Annexes A2, A3, and A4 to the Code). The compatible provisions were grouped into 'Rules of conduct' and attached to the amended data protection Code (Annex A) – see paragraph 5.4.4. This exercise was also carried out with regard to the 'Code of practice applying to the processing of personal data in connection with journalistic activities', leading to the adoption of 'Rules of conduct applying to the processing of personal data in connection with journalistic activities' (Chapter 8). The multi-step revision process concerning other codes of practice and conduct (as contained in Annexes A.5 and A.7 to the former data protection Code) was also started pursuant to Section 20(1) of legislative decree No. 101/2018 (see paragraph 14.3).

Furthermore, a non-exhaustive list of cross-border processing activities subject to mandatory data protection impact assessment was also set out (see decision No. 467 of 11 October 2018), without prejudice to the guidance provided by the 'Article 29' Working Party in the 'Guidelines on data protection impact assessment' as last revised on 4 October 2017 and endorsed by the European Data Protection Board on 25 May 2018 (WP248, rev. 01).

Further clarification was provided concerning qualifications and activities of data protection officers, following the initiatives that had been implemented in 2017 – by way of ad-hoc meetings involving both public sector and private sector stakeholders (see paragraphs

quello privato (cfr. par. 14.1), come pure nell'ambito di iniziative di più ampio respiro (cfr. par. 24.4).

1.5. La ricerca del corretto bilanciamento tra esigenze di trasparenza e diritto alla protezione dei dati personali continua ad occupare una posizione rilevante nell'attività del Garante, come evidenziato dai numerosi pareri resi ai Responsabili per la trasparenza e per la prevenzione della corruzione e ai difensori civici rispetto alla materia dell'accesso civico (par. 4.2.1); materia questa rispetto alla quale la stessa Autorità è risultata destinataria di numerose istanze nel corso del 2018 (par. 26.4).

In questo medesimo ambito deve essere ricordata la recente sentenza della Corte costituzionale del 23 gennaio 2019, n. 20, con la quale è stata dichiarata l'illegittimità costituzionale, per violazione del principio di ragionevolezza e del principio di eguaglianza, dell'art. 14, comma 1-*bis*, d.lgs. 14 marzo 2013, n. 33 (Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni), nella parte in cui prevede, in relazione a tutti i titolari di incarichi dirigenziali, che le pubbliche amministrazioni pubblichino i dati di cui all'art. 14, comma 1, lett. *f*), dello stesso decreto legislativo – ossia una dichiarazione concernente i diritti reali su beni immobili e su beni mobili iscritti in pubblici registri, le azioni di società, le quote di partecipazione a società e l'esercizio di funzioni di amministratore o di sindaco di società, nonché la copia dell'ultima dichiarazione dei redditi, con obblighi estesi al coniuge non separato e ai parenti entro il secondo grado, ove gli stessi vi abbiano consentito e salva la necessità di dare evidenza al mancato consenso. Traendo spunto da tale pronuncia, il Presidente del Garante ha evidenziato che essa "indica con nettezza un percorso virtuoso di bilanciamento tra la protezione dei dati personali e gli altri interessi costituzionalmente rilevanti, che alla

5.4.3 and 14.1, respectively) and within the framework of wider-range initiatives (see paragraph 24.4).

1.5. Striking the right balance between transparency and personal data protection remains one of the topmost commitments for the Italian SA. This is shown by the many opinions rendered on FOIA-type access requests to Transparency and Anti-Corruption Officers as well as to Ombudspersons (paragraph 4.2.1). Indeed, the SA itself received several FOIA-type access requests throughout 2018 (paragraph 26.4).

Reference should be made in this respect to the recent judgment by Italy's Constitutional Court (No. 20 of 23 January 2019), whereby Section 14(1-a) of legislative decree No. 33 of 14 March 2013 was found to be unconstitutional because in breach of reasonableness and equality principles. The said decree regulates FOIA-type access rights and the transparency, publicity, and disclosure obligations applying to public administrative bodies. The provisions at issue envisage that public administrative bodies must publish the information referred to in Section 14(1), letter f), of the decree with regard to all senior officials – i.e., a statement concerning rights in rem on immovable property and registered movable property, any stock or corporate interests held, and any positions covered as members of the board of directors or auditors for any company along with a copy of the latest income statement. This requirement also applies to unseparated spouses and second-degree relatives subject to their consent, whereby non-consent must be documented. When commenting this judgment, the President of the Italian SA remarked that it 'clearly points to a good practice in reconciling personal data protection and other interests as protected by the Constitution, whenever such interests happen to be in conflict with the former as part of public policies'. The President of the SA also criticised certain legislative measures, whether recent or not, which feature

1

prima possano contrapporsi nell'ambito delle politiche pubbliche", stigmatizzando le iniziative legislative, anche recenti, dalle quali traspare invece "una certa insofferenza" al richiamo del Garante "al rispetto del principio di proporzionalità che deve governare il bilanciamento tra diritti, libertà e altri beni giuridici primari", auspicando per il futuro il "ricorso a un supplemento di prudenza, seguendo l'indirizzo tracciato dalla Corte, nel segno del principio di ragionevolezza" (doc. web n. 9084440). I medesimi rilievi erano stati peraltro formulati in passato proprio sulla disciplina di trasparenza (cfr. Relazione 2013, p. 27 ss. e Relazione 2016, p. 15 s., ed ivi ulteriori richiami) e su altri ambiti nei quali interventi legislativi prefiguravano un processo di centralizzazione delle raccolte di dati personali – finanche riferiti alla totalità della popolazione, pure con riguardo agli aspetti più intimi della vita quotidiana –, come nel caso della Piattaforma nazionale dati (cfr. Relazione 2017, p. 37, sulla quale il Garante ha ribadito le proprie riserve nel provv. 22 maggio 2018, n. 31, doc. web n. 9163359) o per i trattamenti effettuati dall'Istat (cfr. Relazione 2017, p. 71, aspetto sul quale si torna al par. 6.2).

1.6. Preoccupazioni che ancora permangono (cfr. par. 3.3), in questo scorcio iniziale del 2019, ed anzi si sono nuovamente riproposte con riguardo alle modalità di attuazione dell'obbligo generalizzato di fatturazione elettronica (iniziativa già intrapresa nella trascorsa legislatura), sul quale ampiamente si sofferma il par. 4.5.2. Ad esse vanno aggiunti, anche in tempi recenti, i richiami indirizzati al legislatore per il rispetto del principio di proporzionalità: ad esempio, nella memoria presentata dal Presidente del Garante nell'ambito del d.d.l. di conversione in legge del decreto-legge 28 gennaio 2019, n. 4, recante disposizioni urgenti in materia di reddito di cittadinanza e di pensioni (A.S. 1018) presentata l'8 febbraio 2019 alla Commissione permanente 11 del Senato della Repubblica (doc. web n.

'some scoffing' at the SA's call for 'respect of the proportionality principle, which must underlie any balancing between rights, freedoms and other primary goods'; he hoped that 'additional care' would be taken in future 'following the lead of the Court, in line with the reasonableness principle'. The same considerations had actually been made in the past exactly regarding transparency legislation (see the 2013 Annual Report, p. 27 and ff., and the 2016 Annual Report, p. 15 and ff.) as well as in respect of other items of draft legislation that envisaged the centralised collection of personal data – in some cases involving the whole of Italy's population and affecting the most intimate sphere of one's life. This is the case, in particular, of the 'National Data Platform' (see the 2017 Annual Report, p. 37, on which the SA's concerns were reiterated in a decision dated 22 May 2018, No. 31) as well as of the processing operations performed by Italy's National Statistics Institute (ISTAT) (see the 2017 Annual Report, p. 71; the issue is mentioned in paragraph 6.2 of this year's Annual Report).

1.6. Those concerns continued in the first months of 2019, indeed additional concerns were raised in connection with implementation of blanket electronic invoicing (e-invoicing) obligations – see paragraph 4.5.2 for further details. Reference should also be made to the call recently made upon Parliament to ensure respect for the proportionality principle - for instance, in the brief submitted by the President of the SA with regard to the bill intended to enact decree-law No. 4 of 28 January 2019, which contained urgent measures on introducing the universal basic income and regulating retirement benefits. The brief was submitted on 8 February 2019 to the XI permanent committee of the Senate; an additional brief was lodged on 6 March 2019 with the joint XI and XII committees of the Chamber of Deputies, taking note of the amendments made – as requested –

9081679) – tema sul quale è tornata la successiva memoria presentata il 6 marzo 2019 alle Commissioni permanenti riunite XI e XII della Camera dei deputati, dando atto degli (auspicati) interventi correttivi apportati nel corso dell'*iter* di conversione del decreto in legge (doc. web n. 9089070) –, come pure in occasione dell'audizione del Presidente del Garante del 6 febbraio 2019, tenutasi nell'ambito dell'esame del disegno di legge A.C. 1433, recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo presso le Commissioni riunite I e XI della Camera dei deputati (doc. web n. 9080870).

Ancora una volta sono i pilastri della disciplina di protezione dei dati personali, da ultimo richiamati anche dalla Corte costituzionale e contenuti nella Convenzione n. 108 del Consiglio d'Europa prima ancora che nelle discipline di diretta derivazione dall'Unione europea, che vengono scossi, non di rado all'insegna della ricerca dell'efficienza dell'azione amministrativa: i principi di pertinenza e non eccedenza (proporzionalità) e quello di finalità. Non può allora che essere salutata con favore, e deve poter dare frutto, l'innovazione contenuta nell'art. 36, par. 4 del RGPD – recante l'obbligo di consultazione dell'autorità di controllo "durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento" (ancorché nell'ordinamento nazionale già da tempo, in concreto, più volte utilmente sperimentata nei rapporti tra l'Autorità e Parlamento e Governo) – che vede nel Garante un *partner* istituzionale essenziale affinché la modernizzazione del Paese, attraverso il potenziamento delle sue infrastrutture digitali, possa aver luogo nel rispetto dei diritti individuali e delle libertà fondamentali.

in the enactment process of the said decree-law. The same call for proportionality was made by the President of the SA during the public hearing held on 6 February 2019 before the joint I and XI committees of the Chamber of Deputies, in connection with the bill containing measures to ensure effectiveness of public administrative activities and to prevent absenteeism.

Once again, it is the pillars of personal data protection that are impacted, which is not infrequently accounted for by the alleged need to achieve effectiveness of administrative activities. Those pillars are made up by the principles of relevance and proportionality along with the purpose limitation principle - as recalled of late by the Constitutional Court and set forth in Council of Europe's Convention 108 already prior to being enshrined in EU-related legislation. This is why one cannot but welcome the innovation brought about by Article 36(4) of the GDPR and hope that it will bear its fruits – namely, the obligation to consult the supervisory authority 'during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing'. Indeed, this exercise has already been carried out successfully at domestic level several times over the past years in terms of the relationships between the SA, Parliament and the Government. The underlying rationale is to consider the Italian SA a fundamental institutional partner in order to make sure that the modernisation of Italy as based on an enhanced digital infrastructure can take place in full compliance with personal rights and fundamental freedoms.

2 Il quadro normativo in materia di protezione dei dati personali

2.1. *Le novità normative con riflessi in materia di protezione dei dati personali*

Il 28 dicembre 2017, con l'adozione del decreto di scioglimento delle Camere da parte del Presidente della Repubblica, si è conclusa la XVII legislatura; con la prima assemblea delle Camere neo-elette, che si è tenuta il 23 marzo 2018, secondo quanto prescritto dall'art. 61, comma 2, della Costituzione, ha preso avvio la XVIII. In ragione dei tempi necessari alla composizione della compagine di governo, nei primi mesi hanno operato solo le Commissioni speciali istituite presso Camera e Senato per l'esame degli atti urgenti del Governo, la cui ultima convocazione si è avuta il 20 giugno 2018.

Terminata l'attività delle Commissioni speciali, si è proceduto alla costituzione delle Commissioni permanenti le quali hanno svolto un'intensa attività di esame nel merito di proposte e disegni di legge o consultiva su atti del Governo, molti dei quali di interesse per l'Autorità sotto il profilo della protezione dei dati personali. Fra i provvedimenti normativi più importanti adottati all'inizio della legislatura, e rispetto ai quali proprio le Commissioni speciali hanno formulato il parere di competenza, va qui menzionato il decreto legislativo 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del RGPD (in G.U. 4 settembre 2018, n. 205).

2.1.1. Il decreto legislativo 10 agosto 2018, n. 101 e le linee di fondo dell'adeguamento della normativa nazionale al RGPD

Decreto legislativo n. 101/2018

Il decreto legislativo n. 101/2018, finalizzato ad adeguare il quadro normativo nazionale alle disposizioni del RGPD, è stato adottato ai sensi dell'art. 13 della legge di delegazione europea 25 ottobre 2017, n. 163, in base ai seguenti criteri: abrogare espressamente le disposizioni del Codice in materia di trattamento dei dati personali incompatibili con le disposizioni contenute nel predetto RGPD; modificare il Codice limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel RGPD; coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal medesimo RGPD; prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante; adeguare, nell'ambito delle modifiche al Codice il sistema sanzionatorio penale e amministrativo vigente con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

Oltre a quelli appena descritti, il decreto è stato conformato al criterio del riassetto e (del)la semplificazione normativa con l'indicazione esplicita delle norme abrogate cui si riferisce l'art. 32, l. 24 dicembre 2012, n. 23, richiamato dal predetto art. 13 della legge-delega.

In relazione all'elaborazione del testo, con decreto del Ministro della giustizia 14 dicembre 2017, è stata istituita una Commissione di studio che ha proceduto alla stesura di una bozza di decreto conformemente ai descritti criteri. In particolare, la Commissione – come può leggersi nella relazione illustrativa allegata allo schema presentato alle competenti Commissioni parlamentari per il parere (A.G. 22) –, a

seguito delle verifiche compiute, ha constatato che la gran parte delle disposizioni del Codice fosse da abrogare espressamente per incompatibilità con quelle contenute nel RGPD, che, a loro volta, sono per la maggior parte direttamente applicabili e costituiscono il regime primario interno circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Altre previsioni codicistiche nazionali sono state modificate, alcune anche in modo rilevante, in relazione a disposizioni del RGPD non direttamente applicabili e che lasciano spazi all'intervento degli Stati membri tramite il legislatore nazionale (artt. 6, par. 2, 9, par. 4, e Titolo IX, del RGPD). Del resto, le numerose clausole di flessibilità contenute nel RGPD hanno reso l'intervento del legislatore nazionale ancor più determinante, caricandolo di responsabilità rispetto al bilanciamento tra gli interessi giuridici coinvolti.

Nonostante i descritti risultati delle verifiche e le indubbie difficoltà di natura squisitamente tecnico-redazionale, il Governo ha deciso di operare essenzialmente all'interno del Codice vigente, in chiave, quindi, di sua novellazione. Questa scelta si spiega peraltro in ragione delle peculiarità del Codice, che essendo stato emanato in tempi relativamente recenti, già conteneva una disciplina avanzata e, per questo, in molti punti collimante o comunque compatibile con il RGPD.

Cionondimeno, proprio la trasversalità della materia e l'esigenza di garantire certezza normativa hanno reso necessario un intervento ampio, informato al criterio direttivo del "riassetto" (che, come anticipato, il citato art. 32, l. n. 234/2012 ammette per le deleghe previste dalla legge di delegazione europea); intervento che ha tenuto conto altresì dell'ulteriore complessità determinata dal sovrapporsi in tale materia di diverse discipline: il RGPD, la direttiva 2016/680 e, in particolare, il relativo decreto legislativo di recepimento 18 maggio 2018 n. 51, che ha espunto dal Codice la disciplina dei trattamenti per fini di polizia e di giustizia penale (cfr. al riguardo il par. 2.2). Sempre dalla relazione illustrativa possono ricavarsi le principali scelte di merito effettuate dal Governo che, perseguendo l'obiettivo della chiarezza e della semplificazione, ha evitato di duplicare alcune disposizioni, molto simili ma non coincidenti, presenti sia nel RGPD che nel Codice ed ha abrogato le corrispondenti disposizioni nazionali ove la materia era già disciplinata dal Regolamento. E ciò sul presupposto che Codice e RGPD sono informati a due filosofie diverse e che quest'ultimo è basato sulla cd. *accountability* (termine tradotto in italiano con responsabilizzazione), in base alla quale il legislatore europeo, in molti casi, rimette la scelta connessa alle caratteristiche principali del trattamento (ivi comprese le misure a protezione degli interessati) al titolare del trattamento che è chiamato ad effettuare una valutazione, ad assumere una decisione e a dare prova di avere adottato misure proporzionate ed efficaci.

Fra le scelte più importanti effettuate dal Governo aventi impatto sulle competenze e sulle attività del Garante, risaltano quella di fare salvi – in una logica di continuità e per un periodo transitorio – i provvedimenti generali e le autorizzazioni al trattamento dei dati sensibili adottati dall'Autorità (v. par. 5.4.4), oggetto in ogni caso di successivo riesame, nonché i codici di deontologia e di buona condotta vigenti, che restano fermi nell'attuale configurazione nelle materie oggetto di riserva normativa degli Stati membri, mentre possono essere, negli altri ambiti, riassunti e modificati su iniziativa delle categorie interessate quali codici di condotta, alla stregua del RGPD (art. 40); la scelta di rafforzare il meccanismo delle consultazioni pubbliche e il coinvolgimento delle categorie interessate in molteplici casi; l'attribuzione al Garante della potestà di promuovere modalità semplificate di adempimento degli obblighi del titolare del trattamento in considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese.

Lo schema del provvedimento, approvato in via preliminare e "salvo intese" dal Consiglio dei ministri il 21 marzo 2018, è stato assegnato il successivo 14 maggio alle Commissioni speciali di Camera e Senato che, in data 20 giugno 2018, hanno espresso il previsto parere (favorevole con condizioni e osservazioni).

Quasi contestualmente (10 maggio), la Presidenza del Consiglio dei ministri – Dipartimento affari giuridici e legislativi ha trasmesso il testo al Garante che ha espresso il parere di competenza con provvedimento 22 maggio 2018, n. 312 (doc. web n. 9163359; cfr. par. 2.1.3 e 3.3.1), formulando alcune osservazioni (accompagnate in alcuni casi da proposte di modifica puntuali delle disposizioni) volte a rendere il decreto pienamente conforme alle disposizioni del RGPD.

Lo schema finale è stato sottoposto all'esame definitivo nel Consiglio dei ministri in data 8 agosto 2018 e il testo approvato, il decreto legislativo n. 101/2018, è entrato in vigore il 19 settembre successivo.

2.1.2. La struttura del decreto legislativo e le sue peculiarità

Il decreto è suddiviso in sei Capi e si compone di 28 articoli, dedicati a specifici aspetti della materia: i Capi da I a IV (artt. da 1 a 16), con tecnica novellistica apportano al Codice le modifiche necessarie ad assicurarne la conformità al RGPD, abrogando le disposizioni incompatibili, modificandone altre e inserendo in alcuni casi nuove disposizioni in esecuzione delle riserve normative previste dal RGPD (cfr. par. 2.1.1); i Capi V e VI riguardano invece la parte extracodicistica dell'intervento normativo. Il Capo V, sotto la rubrica "Disposizioni processuali", consta di un solo articolo, il 17, che, titolato "Modifiche all'articolo 10 del decreto legislativo 1° settembre 2011 n. 150", disciplina e chiarisce, sotto il profilo strettamente procedurale, l'*iter* per dirimere le controversie previste dall'art. 152 del Codice, riformulando l'art. 10, d.lgs. n. 150/2011 sulle suddette controversie in materia di protezione dei dati personali, in modo da avere in tale ambito una disciplina completa del ricorso giurisdizionale previsto dal RGPD. Il Capo VI, infine, è dedicato alle "Disposizioni transitorie, finali e finanziarie" (artt. 18-28).

Più in dettaglio, il Capo I e il Capo II intervengono sul titolo, sulle premesse e sulla Parte I del Codice modificando la rubrica del Titolo I (ora "Disposizioni generali") e introducendo quattro nuovi Capi: "Oggetto, finalità e Autorità di controllo", "Principi", "Disposizioni in materia di diritti dell'interessato", "Disposizioni relative al titolare del trattamento e al responsabile del trattamento".

Il Capo I del Codice contiene, innanzitutto, gli artt. 1 e 2 "Oggetto" e "Finalità" il cui contenuto è innovato rispetto ai corrispondenti articoli previgenti: l'art. 1, nel precisare che il trattamento dei dati personali avviene secondo le norme del RGPD e del Codice, ribadisce i principi generali affermati nella Carta dei diritti fondamentali dell'Unione europea: il rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona; l'art. 2 chiarisce che il Codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del RGPD. Nel medesimo Capo è stato inserito il nuovo art. 2-*bis* il quale individua nel Garante l'autorità nazionale di controllo di cui all'art. 51 del RGPD.

Di seguito al predetto art. 2-*bis*, il decreto legislativo inserisce nel Codice gli artt. da 2-*ter* a 2-*septiesdecies*, mentre gli artt. da 3 a 45, d.lgs. n. 196/2003 vengono abrogati.

In sostanza la Parte I del Codice è profondamente innovata sotto il profilo sistematico, ma molte delle regole presenti nel previgente Codice sono confermate, benché in alcuni casi rimodulate, in conformità al RGPD.

Il Capo II detta i principi generali del trattamento, indicando altresì condizioni e requisiti specifici per categorie particolari di trattamento. Di particolare impor-

tanza è l'art. 2-*ter* il quale (oltre a "confermare" sostanzialmente le definizioni di "comunicazione" e "diffusione" contenute nel Codice previgente) stabilisce che, per quanto riguarda i trattamenti effettuati per "l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri", la base giuridica per i trattamenti aventi ad oggetto dati personali "comuni" sia da rinvenirsi esclusivamente in una norma di legge o di regolamento. L'articolo si presenta come una riformulazione del previgente art. 19 del Codice, confermando che la comunicazione tra soggetti "pubblici" di dati comuni è consentita anche quando manchi una disposizione *ad hoc*, purché la menzionata comunicazione sia necessaria per lo svolgimento di un compito di interesse pubblico o comunque per funzioni istituzionali, salvo che il Garante entro 45 giorni dalla necessaria consultazione abbia adottato una diversa determinazione in termini di garanzie per gli interessati.

L'ambito di applicazione soggettivo della norma viene però esteso al fine di adeguarsi all'impostazione adottata dal RGPD. In quest'ultimo, infatti, scompare la distinzione basata sulla natura pubblica o privata dei soggetti che trattano i dati, rilevando unicamente la finalità del trattamento perseguita, vale a dire se essa concerna un interesse pubblico o privato. L'articolo deve quindi intendersi applicabile ai soggetti che trattano i dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a prescindere dalla loro natura soggettiva (art. 6, par. 1, lett. *e*), del RGPD).

In relazione al trattamento di particolari categorie di dati, già definiti "sensibili" dal Codice previgente, viene invece stabilito l'obbligo di previsione normativa ed è individuato un elenco di trattamenti che si considerano effettuati per "motivi di interesse pubblico rilevante" (art. 2-*sexies* in relazione all'art. 9 del RGPD). Il regime normativo per tali trattamenti è sostanzialmente rimasto inalterato rispetto a quello previsto dal Codice per i trattamenti effettuati da soggetti pubblici (art. 20) e, in particolare, l'elenco predetto è tratto dalle diverse disposizioni del Codice riferite ai trattamenti effettuati per finalità di rilevante interesse pubblico (ad es. artt. 64-73, che il decreto legislativo ha abrogato). Ovviamente, mutato il criterio per delimitare l'ambito applicativo di tale regime, le disposizioni in parola riguardano i trattamenti effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a prescindere dalla natura soggettiva del titolare del trattamento.

Con riferimento ai dati genetici, biometrici e relativi alla salute, oggetto di specifica "riserva" normativa nazionale (cfr. art. 9, par. 4, del RGPD), viene previsto che il relativo trattamento è subordinato anche al rispetto di misure di garanzia disposte dal Garante (art. 2-*septies*). Infine, il trattamento di dati concernenti condanne penali e reati (che trovano nei "dati giudiziari" del Codice il loro "antecedente") è consentito nei limiti di quanto previsto da norme di legge o di regolamento (art. 2-*octies*; cfr. già art. 21, d.lgs. n. 196/2003).

L'art. 2-*decies* conferma l'inutilizzabilità dei dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali (cfr. art. 12, comma 2, d.lgs. n. 196/2003, abrogato), come pure nell'art. 2-*quater* è fatta salva l'adozione di "regole deontologiche" negli ambiti in cui il RGPD riserva la materia agli Stati membri (trattamenti necessari per adempiere un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; trattamento di dati genetici, biometrici o relativi alla salute; talune specifiche situazioni di trattamento di cui al Capo IX, come il rapporto di lavoro ad esempio, o la manifestazione del pensiero e l'attività giornalistica). Tale disposizione trova la propria *ratio* nella scelta di conservare le regole stabilite nei codici di deontologia e di buona condotta previsti all'art. 12 del previgente Codice, che hanno costituito una rile-

vante fonte di riferimento per i settori a cui sono diretti; ciò, però, solo nelle materie oggetto di “riserva” normativa interna agli Stati membri (art. 6, par. 2, del RGPD).

Una novità è rappresentata dall’art. *2-quinquies* che delinea le condizioni specifiche per la validità del consenso prestato dal minore in relazione ai servizi della società dell’informazione.

Il Capo III concerne i diritti garantiti all’interessato la cui disciplina è ora quasi integralmente contenuta nel RGPD. Sulla falsariga di quanto previsto dall’art. 8 del Codice previgente, sono previste limitazioni dei diritti in caso di concreto pregiudizio per altri interessi normativamente tutelati (antiriciclaggio, sostegno delle vittime di atti estorsivi, attività delle commissioni parlamentari d’inchiesta, controllo dei mercati finanziari e monetari, ragioni di giustizia) (artt. 2-*undecies* e 2-*duodecies*).

Alcuni aspetti innovativi presenta, invece, rispetto alla corrispondente disposizione del Codice previgente (art. 9, comma 3), l’art. 2-*terdecies*, concernente il trattamento relativo ai dati di persone decedute, che attribuisce l’esercizio dei diritti dell’interessato a chi abbia un interesse proprio o agisca a tutela dell’interessato o per particolari ragioni familiari, ma anche al mandatario.

Il Capo IV reca disposizioni volte a precisare taluni poteri e obblighi in capo al titolare e al responsabile, tra cui la possibilità di attribuire specifici compiti e funzioni a persone fisiche operanti sotto la loro autorità e responsabilità (art. 2-*quaterdecies*). In relazione all’importante adempimento della valutazione di impatto sulla protezione dei dati previsto a carico del titolare (art. 35 del RGPD) il successivo art. 2-*quinquiesdecies* stabilisce che, con riguardo ai trattamenti svolti per l’esecuzione di un compito di interesse pubblico che possano risultare a rischio elevato, il Garante possa, sulla base di quanto disposto dall’art. 36, par. 5, del RGPD e con provvedimenti di carattere generale adottati d’ufficio, prescrivere misure e accorgimenti a garanzia dell’interessato, che il titolare è tenuto ad adottare.

Nella Parte II del Codice, su cui interviene il Capo III e gli artt. da 3 a 12 del decreto legislativo, viene invece mantenuta inalterata la numerazione degli articoli. Molti vengono modificati, come pure alcune rubriche di Titoli o Capi; altri sono abrogati (ad es. quelli relativi ai trattamenti effettuati per ragioni di giustizia o da Forze di polizia per finalità di prevenzione e repressione di reati – artt. 46-49 e 53-57 – che hanno trovato la loro “collocazione”, *ratione materiae* e con i dovuti adeguamenti, nel decreto legislativo n. 51/2018 di attuazione della direttiva 2016/680).

Analoga impostazione per la Parte III del Codice cui si riferisce il Capo IV dello schema (artt. 13-16), concernente la struttura organizzativa e le funzioni del Garante, le forme di tutela degli interessati e il quadro sanzionatorio (artt. da 140-*bis*, di nuova introduzione, a 172 del Codice).

Significative modifiche sono apportate alle disposizioni relative alla tutela (amministrativa e giurisdizionale) dell’interessato ed alla disciplina sanzionatoria amministrativa per le violazioni della normativa in materia di dati personali: ferme le sanzioni stabilite dal RGPD, sono previste ulteriori sanzioni rispetto ad una serie di violazioni delle disposizioni del Codice stesso (art. 166 come modificato).

Risulta modificata la disciplina del reclamo, unica forma di tutela prevista dal RGPD, per la cui definizione è indicato il termine di nove mesi ovvero dodici mesi in presenza di motivate esigenze istruttorie.

Per quanto riguarda il quadro sanzionatorio, a fronte di elevatissime sanzioni amministrative previste dal RGPD, il decreto legislativo non ha mantenuto alcune delle sanzioni penali che avrebbero potuto sovrapporsi a quelle amministrative, con il conseguente rischio di violazione del divieto del *bis in idem*.

Sotto il profilo sanzionatorio penale, è stato così rimodulato l’impianto delle fat-

tispecie del reato di "trattamento illecito di dati" di cui all'art. 167 del Codice, pur continuando ad essere punibili diverse condotte consistenti nell'arrecare nocumento all'interessato, in violazione di specifiche previsioni indicate nei primi tre commi dell'articolo.

I nuovi commi 4 e 5 consentono la cooperazione tra autorità giudiziaria e Garante, competente per l'irrogazione delle sanzioni amministrative eventualmente coincidenti con l'area della rilevanza penale.

Da questo punto di vista, si apprezza la disposizione del comma 6 (mutuata, si legge nella relazione, dall'art. 187-*terdecies*, d.lgs. n. 58/1998) volta a disciplinare la possibile convergenza sul medesimo fatto di sanzioni penali e amministrative.

Gli artt. 167-*bis* e 167-*ter* introducono nuove fattispecie di reato, concernenti la "Comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone" e la "Acquisizione fraudolenta di dati personali", declinate in relazione a un numero rilevante di persone offese e volte a completare l'apparato delle sanzioni penali nella materia. Alle fattispecie di cui agli artt. 167-*bis* e 167-*ter*, peraltro, si applicano le disposizioni di cui ai commi 4, 5 e 6 del novellato art. 167 appena descritte.

Viene confermata la fattispecie di cui all'art. 168 (Falsità nelle dichiarazioni al Garante), in quanto sanziona condotte caratterizzate da significativo disvalore, con la soppressione però del riferimento alle "notificazioni" al Garante, istituto non più previsto dal RGPD. Al comma 2 dell'art. 168 è aggiunta un'altra fattispecie riferita alla condotta di interruzione o turbativa della regolarità di un procedimento innanzi al Garante o degli accertamenti svolti dall'Autorità. Per "scongiurare" l'ipotesi di una configurabilità del reato a titolo di dolo eventuale, si è introdotto l'avverbio "intenzionalmente" che assicura una peculiare pregnanza alla fattispecie in esame.

Risulta abrogata, invece, la fattispecie di cui all'art. 169 in tema di misure minime di sicurezza, non contemplate dal RGPD. La violazione delle disposizioni in materia di sicurezza sarà sanzionata con misure di carattere amministrativo-pecuniario, ai sensi degli artt. 83 e 5 del RGPD.

Confermato pure l'illecito di cui all'art. 171 quale presidio posto a tutela di beni di particolare rilevanza (controllo a distanza dei lavoratori e divieto di indagini sulle loro opinioni ai sensi degli artt. 4 e 8 dello Statuto dei lavoratori).

*2.1.3. Gli interventi del Garante nel corso dell'*iter *di approvazione del decreto: il parere e l'audizione in Parlamento*

Con il parere reso (provv. 22 maggio 2018, n. 312, doc. web n. 9163359: cfr. par. 3.3.1), il Garante è intervenuto innanzitutto sulla configurazione dei nuovi illeciti penali previsti nello schema di decreto. Al riguardo, ha invitato a definire il novero dei soggetti attivi dei reati previsti (artt. 167, 167-*bis* e 167-*ter*), confermando il ricorso alla locuzione "chiunque", e, con riferimento all'elemento soggettivo, ha evidenziato l'opportunità di considerare nelle fattispecie di illecito sopra descritte, nel dolo specifico, oltre al profitto, anche il danno, in ragione dell'esigenza di presidiare con la sanzione penale condotte connotate da un simile disvalore anche quando sorrette dal dolo di danno e non solo da quello di profitto. Sono state altresì espresse forti riserve rispetto all'abrogazione dell'art. 170, recante il delitto di inosservanza di provvedimenti del Garante, prospettata nella bozza originaria del decreto, a fronte della contestuale introduzione di una figura di reato corrispondente nel decreto legislativo n. 51/2018, limitatamente ai trattamenti svolti per fini di giustizia penale e polizia. Tale disparità di trattamento avrebbe determinato l'insorgere di perplessità in ordine al rispetto del principio di eguaglianza-ragionevolezza, dal momento che alla medesima condotta, lesiva dello stesso bene giuridico

(la piena effettività delle funzioni del Garante), si sarebbero applicati due regimi sanzionatori diversi, solo in ragione della natura soggettiva del titolare e del contesto del trattamento (attività di polizia o giustizia penale, oppure ogni altro ambito). Elementi, questi, inidonei a giustificare, per sé soli, tale differente regime sanzionatorio. L'Autorità ha contestualmente suggerito – in caso di conferma, come poi è avvenuto, della vigenza dell'art. 170 – di individuare gli specifici provvedimenti del Garante la cui inosservanza integri gli estremi del delitto, al fine di conferire alla fattispecie maggiore tassatività.

Le descritte indicazioni dell'Autorità concernenti il quadro sanzionatorio penale sono state recepite dal Governo e, non diversamente (pressoché integralmente) altre che hanno riguardato diversi profili del trattamento dei dati. Ci si riferisce, in particolare, alle condizioni o osservazioni espresse dal Garante in tema di illeciti amministrativi e sanzioni pecuniarie disciplinate nell'art. 166 del decreto, in ordine al quale l'Autorità ha suggerito di includere tra le condotte sanzionabili, anche: a) il mancato svolgimento della valutazione d'impatto e la mancata attivazione, ove necessario, della consultazione preventiva dell'Autorità, nel caso in cui il trattamento di dati sanitari a fini di ricerca medica, biomedica ed epidemiologica sia effettuato in assenza del consenso degli interessati; b) il trattamento ulteriore dei dati a fini di ricerca scientifica o a fini statistici, in assenza della previa autorizzazione del Garante o in violazione della stessa; c) l'omesso riscontro alla richiesta di informazioni o esibizione di documenti al Garante (peraltro già sanzionato dal Codice). Si tratta di adempimenti importanti, la cui omissione è idonea a pregiudicare i poteri di controllo dell'Autorità funzionali alla legittimità dei trattamenti e va pertanto sanzionata anche a fini deterrenti. Fra le indicazioni recepite risultano anche quelle rese dal Garante: in materia di trattamento di "dati particolari" (già "sensibili" in base al previgente Codice) per "motivi di interesse pubblico rilevante" ai sensi dell'art. 9, par. 1, lett. *g*), del RGPD, al fine di riprodurre in maniera sostanzialmente inalterata il regime normativo previsto al previgente articolo 20 del Codice per i trattamenti di dati sensibili effettuati da soggetti pubblici (nuovo art. 2-*sexies* del Codice); in tema di "misure di garanzia" per il trattamento dei dati genetici, relativi alla salute e biometrici, con riferimento più specifico al trattamento dei dati biometrici per finalità di sicurezza, di cui al nuovo art. 2-*septies*; in tema di consenso del minore rispetto ai servizi della società dell'informazione, il Garante ha ritenuto non condivisibile l'indicazione dell'età di sedici anni quale "soglia" legittimante l'espressione consapevole del consenso, poiché non coerente con altre disposizioni dell'ordinamento che individuano, invece, nei quattordici anni il limite di età per esercitare determinati atti (il nuovo art. 2-*quinquies* contiene ora l'espresso riferimento alla soglia dei quattordici anni); relative, infine, all'"ulteriore utilizzo" di informazioni già raccolte per finalità statistica e di ricerca scientifica che il Garante ha ammesso per consentire la ricerca scientifica su dati genetici, ma con le garanzie necessarie per gli interessati e sulla base di una autorizzazione (anche generale) del Garante (art. 110-*bis* del Codice previgente, come modificato dal decreto legislativo n. 101/2018).

Il Governo non ha tenuto conto, invece, nell'elaborazione definitiva del decreto, delle forti preoccupazioni espresse dall'Autorità in materia di conservazione dei dati di traffico telefonico e telematico.

Il novellato art. 132 del Codice conferma infatti la deroga alla disciplina sulla conservazione dei dati di traffico telefonico e telematico, nonché dei dati relativi alle chiamate senza risposta, introdotta dall'art. 24, l. n. 167/2017, che ha prolungato fino a 72 mesi il termine di conservazione di tali delicate informazioni al fine di garantire strumenti di indagine efficaci in considerazione delle straordinarie esi-

genze di contrasto del terrorismo, anche internazionale, nonché per finalità di accertamento e repressione dei pertinenti, gravi reati (di cui agli artt. 51, comma 3-*quater*, e 407, comma 2, lett. *a*), c.p.p.). Il Garante, nel parere, ha osservato che la conferma della predetta deroga avrebbe determinato rilevanti criticità – come già segnalato nel parere 22 febbraio 2018 reso sullo schema di decreto di recepimento della direttiva (UE) 2016/680 (cfr. par. 2.2) – in ordine al rispetto del principio di proporzionalità tra esigenze investigative e limitazioni del diritto alla protezione dei dati dei cittadini, affermato dalla CGUE con le sentenze *Digital Rights Ireland* (resa in data 8 aprile 2014 nelle cause riunite C-293/12 e C-594/12,) e Tele2 e Watson (resa il 21 dicembre 2016, nelle cause riunite C 203/15 e C 698/15). In ragione della incompatibilità della deroga con il principio di proporzionalità (come interpretato dalla Corte di giustizia nelle richiamate sentenze) e al fine di garantire la piena conformità dell'ordinamento interno al diritto dell'Unione europea, l'Autorità pertanto ha chiesto di espungere dallo schema di decreto ogni riferimento al predetto art. 24, l. n. 167/2017 e la sua contestuale abrogazione; ma le indicazioni rese in proposito non hanno avuto seguito.

Il Governo non ha seguito le indicazioni del Garante, ritenendo che l'abrogazione dell'art. 24, l. n. 167/2017 avrebbe riguardato materie estranee all'ambito di stretto adeguamento dell'ordinamento interno al RGPD ed esorbitasse dai limiti della delega legislativa, la quale avrebbe consentito, nella prospettiva del Governo medesimo, solo interventi di mero coordinamento con il quadro normativo vigente. Analoga valutazione, del resto, era stata già compiuta in merito al decreto delegato attuativo della direttiva 680/2016 (cfr. par. 2.2).

Successivamente, nel corso dell'esame del provvedimento normativo da parte delle Commissioni parlamentari speciali, al Garante è stato richiesto di tenere un'audizione innanzi alle Commissioni speciali di Camera e Senato riunite (7 giugno 2018); in tale occasione il Presidente, dopo aver ribadito quanto già ampiamente evidenziato nel parere, ha rilevato come alcune delle criticità emerse nel corso del dibattito parlamentare coincidessero con le osservazioni contenute nel provvedimento dell'Autorità.

Quanto all'introduzione di condizioni ulteriori per il trattamento di dati biometrici, genetici, relativi alla salute, il Garante ha rammentato che essa è espressamente consentita dall'art. 9, par. 4, del RGPD, che per tale sotto-categoria di dati "particolari" ammette una tutela ulteriormente rafforzata, di cui peraltro si è avvalsa la maggior parte dei Paesi membri. Inoltre, il Presidente ha chiesto di valutare l'espressa inclusione, all'interno della categoria dei dati relativi a condanne penali e reati (prevista dall'art. 10 del RGPD), dei dati relativi all'applicabilità delle misure di prevenzione, già ricompresi all'interno dell'omologa, ma superata categoria dei "dati giudiziari" del previgente Codice, e sicuramente meritevoli di una tutela rafforzata, pari a quella riconosciuta agli altri dati di cui all'art. 10, attraverso un'interpretazione estensiva del suo ambito applicativo a misure che non tutti gli Stati membri conoscono. La richiesta integrazione però non è stata "recepita" dalle Commissioni nei relativi pareri e, per l'effetto, dal Governo nel testo definitivo del decreto.

Infine, prendendo spunto da alcune obiezioni espresse da altri soggetti auditi, il Garante ha puntualizzato alcuni aspetti. In ordine all'eccepita assenza di contraddittorio nel procedimento per l'irrogazione di sanzioni amministrative, il Presidente ha chiarito che detto contraddittorio è, invece, espressamente previsto (come già in base al previgente Codice) con la possibilità di depositare memorie e chiedere audizioni (art. 166, comma 7, come modificato), in analogia alla possibilità di presentazione di memorie difensive prevista espressamente dall'art. 18, comma 4, d.lgs. n.

101/2018 nell'ambito della procedura da esperire, in fase transitoria, per la definizione agevolata delle violazioni contestate anteriormente alla data di entrata in vigore del decreto. Quanto poi all'asserita assenza di difesa tecnica nel procedimento amministrativo volto alla definizione dei reclami, è stato precisato che la norma consente comunque un'assistenza tecnica (pur non prevedendola come obbligatoria) e perciò non comporta alcuna limitazione del diritto di difesa esattamente come non la comportava il Codice previgente rispetto ai ricorsi, parimenti alternativi alla tutela giurisdizionale. Al contrario, la previsione della necessaria difesa tecnica costituirebbe una limitazione delle possibilità di esercizio dei diritti incompatibile con il regime di ampia accessibilità ai mezzi di tutela, sancito dall'art. 77 del RGPD, oltre che un onere ulteriore per cittadini e imprese.

2.2. *Il decreto legislativo 18 maggio 2018, n. 51, di attuazione della direttiva (UE) 2016/680 sui trattamenti effettuati a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali*

Sempre con riferimento all'attuazione sul piano nazionale della normativa europea di cui al cd. "pacchetto protezione dati", particolare importanza assume il decreto legislativo 18 maggio 2018, n. 51, di attuazione della direttiva (UE) 2016/680 del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, adottato in base alla legge 25 ottobre 2017, n. 163, recante la delega al Governo per il recepimento delle direttive europee e l'attuazione degli atti dell'Unione europea (legge di delegazione europea 2016/2017).

Il decreto, in linea con le disposizioni della direttiva, ha inteso fornire una regolamentazione organica del trattamento di dati personali effettuato per fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, la quale sostituisce in gran parte quella contemplata nei titoli I e II della parte seconda del Codice. Si è scelto di ridisegnare la regolamentazione del trattamento dei dati personali con riguardo alla sua finalità, piuttosto che in relazione all'autorità competente al trattamento, in ogni caso assicurando le distinzioni rese necessarie dalle diverse caratteristiche e dalla differente natura delle autorità interessate: giudiziaria e di polizia.

In ambito giudiziario, in particolare, la tutela degli interessati viene assicurata dalle garanzie che riconoscono i diritti di difesa all'interno del procedimento penale, assicurando quindi la possibilità di limitare l'esercizio dei diritti degli interessati conformemente alle esigenze di prevenzione, di indagine e processuali. In materia di sicurezza del trattamento, si prevede come obbligatoria anche per l'autorità giudiziaria la nomina del responsabile della protezione dati, in ragione dell'ausilio che tale figura può fornire nella gestione di trattamenti complessi e spesso inerenti a dati di particolare delicatezza. Per quanto riguarda il trasferimento dei dati personali verso Paesi terzi o organizzazioni internazionali, si stabilisce che esso sia consentito solo nei confronti delle autorità competenti e per le finalità di pubblica sicurezza oggetto della direttiva e in presenza di specifiche condizioni, tra le quali l'adozione, da parte della Commissione europea, di una decisione di adeguatezza.

Sullo schema di provvedimento il Garante, individuato dal decreto quale autorità deputata a vigilare sul rispetto delle norme attuative della direttiva in funzione della tutela dei diritti e delle libertà fondamentali delle persone fisiche coinvolte, si

è espresso suggerendo talune modifiche funzionali al perfezionamento del testo in senso conforme alla normativa europea (parere 22 febbraio 2018, n. 312, doc. web n. 9163359, su cui v. anche par. 3.3.1).

Nel parere reso, pur rilevando l'assenza nello schema di criticità rispetto alla garanzia del diritto alla protezione dei dati personali, il Garante ha ritenuto opportuno suggerire alcune modifiche, funzionali al suo perfezionamento, solo in parte accolte. Fra le osservazioni recepite, alcune in materia di informativa, termini di conservazione dei dati e delle registrazioni di operazioni, valutazione di impatto, trasferimenti in Paesi terzi (artt. 10, 21, 23 e 33). È stata poi recepita integralmente anche la proposta di modifica dell'art. 7 dello schema concernente il trattamento dei dati personali "particolari" ai sensi dell'art. 9 del RGPD (già "sensibili" alla stregua del previgente Codice), che pertanto è consentito – come proposto dal Garante – solo se "strettamente necessario". Il Governo non ha ritenuto, invece, di adeguarsi ad altre osservazioni del Garante in tema di illeciti penali ed amministrativi e conservazione di dati di traffico.

Così è stato per le osservazioni relative alla fattispecie delittuosa di cui all'art. 43 "trattamento illecito di dati" nella parte in cui, al fine di contrastare possibili abusi nel ricorso a metodi investigativi particolarmente invasivi (quali i processi decisionali automatizzati di cui all'art. 8 del medesimo decreto), il Garante aveva chiesto di valutare l'opportunità di punire con un trattamento sanzionatorio più rigoroso (quello del comma 2) tutti i casi di violazione della disciplina concernente il divieto di decisioni basate unicamente su un trattamento automatizzato, e non solo l'ipotesi di profilazione discriminatoria con utilizzo di dati "particolari" ai sensi dell'art. 9 del RGPD (già "dati sensibili" alla stregua della disciplina previgente).

Per quanto riguarda gli illeciti amministrativi (art. 42 del decreto), l'Autorità aveva rilevato l'opportunità di prevedere quali cornici edittali quelle comminate dal RGPD, al fine di garantire maggiore omogeneità nella tutela accordata al medesimo bene giuridico nell'ambito dei vari settori oggetto di disciplina, sottolineando che, in assenza di tale correttivo, si sarebbe determinata "una rilevante disparità di trattamento, sotto il profilo sanzionatorio, tra condotte del tutto analoghe, lesive del medesimo bene giuridico, per il solo fatto di essere realizzate in contesti differenti. Peraltro, proprio la circostanza dell'essere tali illeciti realizzati da parte di autorità pubbliche incaricate di funzioni di primaria rilevanza – in quanto incidenti su diritti e libertà fondamentali quali, in primo luogo, la libertà personale – mediante trattamenti caratterizzati da particolare invasività, dovrebbe al contrario legittimare la comminatoria di sanzioni maggiori o comunque analoghe a quelle previste nei settori di competenza del RGPD, non certo inferiori". Tale osservazione non è stata accolta – come si legge nella relazione illustrativa del decreto legislativo – sul presupposto che "al riguardo non è invocabile il disallineamento con analoghe previsioni sanzionatorie del RGPD", e "in mancanza di criteri e principi direttivi specifici, in punto di sanzioni amministrative, rinvenibili nell'art. 11 della legge n. 163/2017, occorre far riferimento ai principi richiamati all'art. 1 della medesima legge, che espressamente rinvia all'art. 32 della legge quadro n. 234/2012. Le sanzioni pecuniarie amministrative, pertanto, non possono superare i limiti massimi ivi previsti, pari a 150.000 euro". Ipotesi di sanzioni pecuniarie amministrative più elevate si scontrerebbe con i limiti della delega legislativa.

Quanto alla *data retention*, il Garante ha segnalato al Governo di inserire nel provvedimento alcune essenziali modifiche alla normativa sulla conservazione dei dati di traffico per fini di giustizia per adeguarla ai principi sanciti dalla Corte di Giustizia UE con mirati interventi sull'art. 132 del Codice e sopprimendo l'art. 24, l. n. 167/2017. Come detto, tali indicazioni (ripetute poi dal Garante nel parere sullo schema di

decreto legislativo di adeguamento al RGPD, per il quale si veda il precedente par. 2.1) sono state disattese dal legislatore in quanto riferite a materie estranee all'ambito di stretta attuazione della direttiva ed esorbitante dai limiti della delega legislativa.

2.3. *Le leggi di particolare interesse per la protezione dei dati personali*

Nel 2018 sono stati approvati numerosi provvedimenti normativi con riflessi sulla protezione dei dati personali. Fra questi, al fine di offrirne una ricognizione, seppur sintetica, comunque tale da rendere conto dell'ampiezza e dell'eterogeneità delle materie che rientrano nell'area di interesse dell'Autorità, si menzionano in particolare:

Misure di contrasto ai reati contro la p.a. e di trasparenza dei partiti e dei movimenti politici

1) la legge 9 gennaio 2019, n. 3, che introduce misure in materia di contrasto ai reati contro la p.a., di prescrizione e di trasparenza dei partiti e dei movimenti politici e delle fondazioni, con particolare riferimento al loro finanziamento. Per quanto riguarda la disciplina della trasparenza dei partiti politici, che ha un notevole impatto sulla protezione dei dati, le nuove disposizioni sono volte a rafforzare gli obblighi di trasparenza sia in ordine ai contributi ricevuti, sia alla presentazione delle candidature. In particolare è previsto, per i partiti e i movimenti politici nonché per le liste e per i candidati alla carica di sindaco che partecipano alle elezioni nei comuni con più di 15.000 abitanti, l'obbligo di annotare – entro il mese successivo a quello della percezione – in un apposito registro, per ogni contributo ricevuto, l'identità dell'erogante, l'entità del contributo o il valore della prestazione o di altra forma di sostegno e la data dell'erogazione. Di particolare interesse sono le disposizioni che prevedono l'obbligo di pubblicare sul sito istituzionale dei partiti i dati identificativi dei sostenitori che abbiano corrisposto contributi, nonché, in occasione delle competizioni elettorali, il certificato penale dei candidati. L'obbligo di trasparenza è riferito alle elargizioni di contributi in denaro complessivamente superiori nell'anno a euro 500 per soggetto erogatore, o di prestazioni o altre forme di sostegno di valore equivalente. Inoltre, in occasione di competizioni elettorali (salvo le elezioni in comuni con popolazione inferiore a 15.000 abitanti) è previsto per i partiti, movimenti politici e liste che si presentano alle elezioni l'obbligo di pubblicare sul proprio sito internet il *curriculum vitae* fornito dai propri candidati ed il relativo certificato penale, rilasciato dal casellario giudiziale non oltre 90 giorni prima della data fissata per le elezioni. I medesimi documenti sono pubblicati in apposita sezione denominata "Elezioni trasparenti" del sito internet dell'ente cui si riferisce la consultazione elettorale. Alcune disposizioni del provvedimento normativo sono state modificate nel corso dell'esame parlamentare in parziale conformità alle indicazioni rese dal Garante nell'audizione richiesta dalle Commissioni affari costituzionali e giustizia della Camera e tenuta il 10 ottobre 2018 (doc. web n. 9049788; cfr. par. 3.1). In tale occasione il Presidente ha ribadito la natura di "dato sensibile" delle informazioni sui contributi forniti a un determinato partito politico o movimento, suscettibili di determinare stigmatizzazioni motivate da avversione politica o ideologica e di essere alimentate dall'indiscriminata diffusione nella rete. Ha, poi, da un lato, richiamato il regolamento (UE) 2014/1141 sul finanziamento dei partiti politici europei e la graduazione delle soglie oltre le quali trovano applicazione gli obblighi di pubblicazione ivi individuati e, dall'altro, espresso forti perplessità sulla generalizzata pubblicazione del certificato penale dei candidati, ritenendola sproporzionata e richiedendo perciò un raccordo tra tale previsione e la disciplina dell'incandidabilità a competizioni elettorali, con una rimodulazione dell'ampiezza della pubblicazione in ragione delle diverse caratteristiche della predetta disciplina per ciascun tipo di elezione.

Tali ultime indicazioni non sono state recepite. Sotto altro profilo, mentre l'Autorità aveva richiesto di individuare termini di pubblicazione obbligatoria dei dati strettamente commisurati e non eccedenti le finalità perseguite, è stato previsto un periodo di pubblicazione dei dati sul sito internet del partito o movimento politico non inferiore a 5 anni, che appare sproporzionato stante peraltro la sua indeterminatezza. Quanto all'obbligo di pubblicare il *curriculum vitae* e il certificato penale dei candidati – aspetto quest'ultimo di maggiore criticità – anche sul sito del Ministero dell'interno, in caso di elezione del Parlamento nazionale o dei membri del Parlamento europeo, e di quello dell'ente cui si riferisce la consultazione elettorale, l'Autorità aveva segnalato l'opportunità di stabilire, anche tramite un regolamento attuativo, modalità di assolvimento di tale obbligo con misure appropriate e specifiche finalizzate a prevedere un accesso selettivo a tali dati (con credenziali rilasciate a chiunque ne abbia interesse e dietro specifica richiesta) ed a renderli disponibili in formato protetto dal rischio di copia o alterazione, per un tempo proporzionato alle esigenze perseguite (ad es., quella della campagna elettorale). Al riguardo, il testo di legge approvato si limita a stabilire che la pubblicazione deve consentire all'elettore di accedere alle informazioni ivi riportate attraverso apposita ricerca per collegio o nominativo del candidato e demanda ad un decreto del Ministro dell'interno la definizione delle modalità tecniche di "acquisizione dei dati su apposita piattaforma informatica".

Legge di bilancio

2) La legge 30 dicembre 2018, n. 145, recante il bilancio di previsione dello Stato per l'anno finanziario 2019 e bilancio pluriennale per il triennio 2019-2021. Tra le disposizioni di interesse per i riflessi sulla protezione dei dati personali si segnalano quelle che istituiscono l'imposta su servizi digitali (cd. web tax), la cui disciplina di attuazione sarà stabilita con decreto del Ministro dell'economia e delle finanze, di concerto con il Ministro dello sviluppo economico, sentito anche il Garante (art. 1, commi 35 e 45). Si segnalano, inoltre, le disposizioni che per finalità di monitoraggio della spesa farmaceutica consentono all'Aifa di avvalersi dei dati contenuti nelle fatture elettroniche e nel Nuovo sistema informativo sanitario, Nsis (commi 576 e 583). Di interesse inoltre le disposizioni in materia di carta di identità elettronica (Cie) e di servizi postali, compresa la possibilità per il Ministero dell'interno di stipulare convenzioni ai fini della riduzione degli oneri amministrativi e di semplificazione delle modalità di richiesta, gestione e rilascio della Cie con soggetti che abbiano particolari requisiti (siano cioè dotati di una rete di sportelli diffusa su tutto il territorio nazionale; siano *identity provider*; abbiano la qualifica di *Certification Authority*) (commi 811, 812 e 813). Il comma 812 apporta al riguardo alcune modifiche conseguenziali al Cad, prevedendo che le caratteristiche e le modalità per il rilascio della Cie non siano più definite con d.P.C.M, ma con decreto del Ministro dell'interno. Infine, un'altra disposizione di interesse (comma 1100), prevede che, a decorrere dal 1° luglio 2019, i titoli di accesso ad attività di spettacolo in impianti con capienza superiore a 5.000 spettatori debbano riportare l'indicazione del nome e del cognome del soggetto che fruisce del titolo di accesso, nel rispetto delle disposizioni in materia di protezione dei dati personali. È inoltre previsto che l'accesso all'area dello spettacolo sia subordinato al riconoscimento personale dei partecipanti all'evento, compresi i minorenni, attraverso controlli e meccanismi efficaci di verifica dell'identità (introduzione dei commi 545-*bis*, 545-*quinquies* all'art. 1, l. n. 232/2016 - Bilancio di previsione dello Stato per l'anno finanziario 2017).

Decreto-legge fiscale

3) Il decreto legge 23 ottobre 2018, n. 119, recante "Disposizioni urgenti in materia fiscale e finanziaria", convertito dalla legge 17 dicembre 2018, n. 136, il cui art. 17, rubricato "Obbligo di memorizzazione e trasmissione telematica dei corrispettivi", rende obbligatoria la memorizzazione elettronica e la trasmissione telema-

2

tica all'Agenzia delle entrate dei dati relativi ai corrispettivi (cd. scontrino fiscale). La previsione è connessa alla cd. lotteria dei corrispettivi, nota anche come lotteria degli scontrini (in ragione dell'estrazione, nell'ambito di una lotteria nazionale, di un premio mensile associato al codice degli scontrini) la cui decorrenza, precedentemente fissata al 1° gennaio 2018, è stata rinviata al 1° gennaio 2020. Sono state inoltre previste disposizioni di semplificazione per l'avvio della fatturazione elettronica (art. 10), con particolare riferimento agli operatori sanitari (art. 10-*bis*) e agli operatori che offrono servizi di pubblica utilità (art. 10-*ter*). Si segnala, infine l'art. 16-*quater* che, al fine di rafforzare le misure volte al contrasto dell'evasione fiscale, prevede che le informazioni registrate nell'archivio dei rapporti finanziari possano essere utilizzate dalla Guardia di finanza, anche in coordinamento con l'Agenzia delle entrate, nonché dal Dipartimento delle finanze.

Disposizioni in materia di sicurezza pubblica

4) Il decreto-legge 4 ottobre 2018, n. 113, recante "Disposizioni urgenti in materia di protezione internazionale e immigrazione, sicurezza pubblica, nonché misure per la funzionalità del Ministero dell'interno e l'organizzazione e il funzionamento dell'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata", convertito dalla legge 1° dicembre 2018, n. 132. Tra le disposizioni di interesse si segnala, in particolare, l'art. 16 (rubricato "Controllo, anche attraverso dispositivi elettronici, dell'ottemperanza al provvedimento di allontanamento dalla casa familiare") che introduce la facoltà di utilizzare il braccialetto elettronico come strumento di controllo dell'esecuzione del provvedimento di allontanamento dalla casa familiare nelle delicate ipotesi in cui si proceda per i delitti di cui all'art. 572 c.p. (Maltrattamenti contro familiari e conviventi) e all'art. 612-*bis* c.p. (Atti persecutori, cd. *stalking*), ossia in situazioni caratterizzate da peculiari profili di pericolosità per l'incolumità personale della persona offesa e che destano particolare allarme sociale. Di interesse è anche l'art. 17 del provvedimento normativo in parola ai sensi del quale gli esercenti l'attività di autonoleggio di veicoli senza conducente devono comunicare i dati identificativi dei clienti al Ced *interforze* del Dipartimento della pubblica sicurezza, al fine di verificare se a loro carico risultino specifici precedenti o segnalazioni delle Forze di polizia relativi a fatti o situazioni rilevanti per la prevenzione del terrorismo. In particolare, si prevede che i dati comunicati siano conservati per un periodo di tempo non superiore a sette giorni e che con decreto del Ministro dell'interno di natura non regolamentare, da adottarsi sentito il Garante, siano definite le modalità tecniche dei collegamenti attraverso le quali sono effettuate le suddette comunicazioni, nonché di conservazione dei dati. Inoltre, l'art. 18 prevede un ampliamento dell'accesso da parte dei Corpi e servizi della polizia municipale, nei comuni con popolazione superiore ai centomila abitanti, a specifici archivi presenti nella banca dati del predetto Ced *interforze*. La consultazione dei dati avviene per il tramite di un sistema/applicazione di risposta "semaforica", del tipo *hit/no hit*, che consente in caso di esito positivo di evidenziare l'eventuale sussistenza, in capo ai soggetti controllati, di provvedimenti "attivi" nel citato sistema informativo, i quali richiedono un seguito operativo, quali i provvedimenti restrittivi della libertà personale, i rintracci degli scomparsi, i provvedimenti adottati in applicazione dell'Accordo di Schengen e quelli inerenti la patente di guida. La norma rinvia, quindi, ad un decreto del Ministro dell'interno, da emanare sentita la Conferenza Stato-città ed autonomie locali e il Garante, la definizione delle modalità di collegamento al Ced e i relativi standard di sicurezza, nonché il numero dei soggetti che ciascun comune può abilitare alla consultazione dei dati. Infine, l'art. 35-*sexies* ha previsto che con decreto del Ministro dell'interno (di concerto con il Ministro della difesa, dell'economia e delle finanze e delle infrastrut-

ture e dei trasporti) siano disciplinate le modalità di utilizzo da parte delle Forze di polizia, di droni ai fini del controllo del territorio per finalità di pubblica sicurezza, con particolare riferimento al contrasto al terrorismo e alla prevenzione dei reati di criminalità organizzata e ambientale.

Proroga del *bonus* cultura ai diciottenni

5) Il decreto-legge 25 luglio 2018, n. 91, recante "Proroga di termini previsti da disposizioni legislative" convertito dalla legge 21 settembre 2018, n. 108, del quale si segnala l'art. 7 che assicura la necessaria copertura legislativa all'estensione per il 2018 del *bonus* cultura per i diciottenni. In relazione a tale beneficio il Garante ha espresso parere su uno schema di d.P.C.M. recante modifiche al decreto 15 settembre 2016, n. 187, sui criteri e le modalità di attribuzione e di utilizzo della carta elettronica prevista dall'art. 1, comma 979, legge 28 dicembre 2015, n. 208, attraverso la quale si fruisce del *bonus* (parere 7 novembre 2018, n. 477, doc. web n. 9058972, cfr. par. 3.3.2).

Nuove disposizioni in materia di iscrizione e funzionamento del Registro delle opposizioni

6) La legge 11 gennaio 2018, n. 5, contenente nuove disposizioni in materia di iscrizione e funzionamento del Registro delle opposizioni a istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato. La legge, approvata definitivamente in Commissione trasporti del Senato il 22 dicembre 2017 e pubblicata in G.U. 3 febbraio 2018, n. 28, introduce alcune significative novità nel panorama normativo in materia di telemarketing, prime, fra tutte, l'obbligo di rendere conoscibile la natura commerciale delle telefonate provenienti dai *call center* e la possibilità di iscrivere nel Registro delle opposizioni anche le numerazioni fuori elenco, comprese quelle di telefonia mobile (art. 1, comma 2). Nel Registro pubblico delle opposizioni, istituito presso il Ministero dello sviluppo economico con d.P.R. 7 settembre 2010, n. 178 e operante dal 2011, potevano essere iscritte, infatti, coerentemente a quanto previsto dall'art. 130, comma 3-*bis*, del Codice, esclusivamente le numerazioni inserite nei pubblici elenchi, restando pertanto escluse le utenze mobili e quelle fisse non iscritte in tali elenchi. Al fine di rendere effettiva la tutela degli utenti, le nuove disposizioni hanno inoltre previsto che con l'iscrizione nel Registro si intendono revocati tutti i consensi precedentemente espressi, con qualsiasi forma o mezzo e a qualsiasi soggetto, ed è altresì precluso l'uso delle numerazioni telefoniche cedute a terzi dal titolare del trattamento sulla base dei consensi precedentemente rilasciati (art. 1, comma 5). Sono tuttavia fatti salvi i consensi prestati nell'ambito di specifici rapporti contrattuali in essere, ovvero cessati da non più di trenta giorni, aventi ad oggetto la fornitura di beni o servizi, per i quali è comunque assicurata, con procedure semplificate, la facoltà di revoca. La nuova legge conferma che l'iscrizione nel Registro è consentita a tutti gli interessati che vogliano opporsi al trattamento delle proprie numerazioni telefoniche effettuato con l'impiego del telefono, mediante operatore, per fini di invio di materiale pubblicitario o di vendita diretta, per il compimento di ricerche di mercato o di comunicazione commerciale. Le nuove disposizioni saranno concretamente operanti dopo l'emanazione di un regolamento attuativo (d.P.R. su proposta del Ministro dello sviluppo economico: art. 1, comma 1, l. n. 5/2018), il cui schema è all'attenzione del Garante, con cui saranno apportate le opportune modifiche alle disposizioni regolamentari vigenti che disciplinano le modalità di iscrizione e funzionamento del Registro (d.P.R. n. 178/2010).

Testimoni di giustizia

7) La legge 11 gennaio 2018, n. 6, recante disposizioni per la protezione dei testimoni di giustizia, il cui art. 5, al fine di assicurare l'incolumità dei testimoni di giustizia e delle altre persone protette e la sicurezza dei loro beni, prevede che possano essere applicate speciali misure tra le quali il mutamento di identità dei testimoni di giustizia da autorizzare con decreto del Ministro dell'interno, di concerto

con il Ministro della giustizia, garantendone la riservatezza anche in atti della pubblica amministrazione.

2.4. *I decreti legislativi*

Nel 2018, oltre alle leggi richiamate nel paragrafo 2.3 e ai due decreti legislativi di adeguamento e attuazione del quadro normativo europeo (cfr. par. 2.1. e 2.2), sono stati approvati altri decreti legislativi aventi riflessi in materia di protezione dei dati personali – sui cui schemi, in alcuni casi, il Garante ha espresso parere – fra i quali si menzionano in particolare:

Casellario giudiziale

– decreto legislativo 2 ottobre 2018, n. 122, recante le disposizioni per la revisione della disciplina del casellario giudiziale, in attuazione della delega di cui all'art. 1, commi 18 e 19, l. 23 giugno 2017, n. 103. In particolare, il decreto – sul cui schema il Garante ha reso parere il 13 settembre 2018 (doc. web n. 9055083, cfr. par. 3.3.1) – adegua la disciplina del casellario alle modifiche intervenute nella materia penale, anche processuale e nel diritto dell'Unione europea in materia di protezione dei dati personali, con l'obiettivo della semplificazione del procedimento e della riduzione degli adempimenti amministrativi;

Pnr

– decreto legislativo 21 maggio 2018, n. 53, recante l'attuazione della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (Pnr) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e disciplina dell'obbligo per i vettori di comunicare i dati relativi alle persone trasportate in attuazione della direttiva 2004/82/CE del Consiglio del 29 aprile 2004. Con il predetto decreto – sul cui schema il Garante ha espresso parere in data 22 febbraio 2018 (doc. web n. 8159625, cfr. par. 3.3.1) – si è inteso disciplinare un ulteriore strumento nelle attività di prevenzione e di contrasto dei reati di terrorismo e di altri reati gravi, ed assorbire la normativa introdotta dalla direttiva 2004/82/CE del 29 aprile 2004 (direttiva Api) recepita con il decreto legislativo 2 agosto 2007, n. 144, che ha introdotto l'obbligo per i vettori aerei di comunicare ai competenti uffici di polizia di frontiera talune informazioni relative alle persone trasportate nel territorio dello Stato (Api). Pertanto, al fine di operare una semplificazione e razionalizzazione del sistema, con il decreto si è evitata la duplicazione di banche dati e di distinti sistemi informativi, provvedendo a disciplinare in modo uniforme i diversi obblighi dei vettori aerei;

Decreto antiriciclaggio

– decreto legislativo 18 maggio 2018, n. 60, concernente l'attuazione della direttiva (UE) 2016/1148 del Consiglio del 6 dicembre 2016, recante modifica della direttiva 2011/16/UE del Consiglio, del 15 febbraio 2011, in materia di accesso da parte delle autorità fiscali alle informazioni utili per finalità antiriciclaggio, al fine di garantire una cooperazione amministrativa efficiente tra gli Stati membri, sul cui schema il Garante aveva espresso parere nel 2017 (parere 9 marzo 2017, n. 125, doc. web n. 6124534);

Direttiva NIS - *Network and Information Security*

– decreto legislativo 18 maggio 2018, n. 65, di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (cd. direttiva Nis - *Network and Information Security*). Tale disciplina è volta a conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea. Il decreto detta la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti

per dare attuazione agli obblighi previsti dalla direttiva 2016/1148 che rappresenta il caposaldo della strategia dell'Unione in materia di sicurezza delle reti e dei sistemi informativi**.** In particolare, il decreto persegue tre obiettivi: 1) promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, in particolare gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali e i fornitori di servizi digitali; 2) migliorare le capacità nazionali di *cybersecurity*; 3) rafforzare la cooperazione a livello nazionale e in ambito UE;

Tutela del *know-how* e informazioni commerciali riservate

– decreto legislativo 11 maggio 2018, n. 63, recante "Attuazione della direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del *know-how* riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti". Il decreto prevede sanzioni penali ed amministrative nonché rimedi cautelari e risarcitori al fine di ridurre il rischio di diffusione di pratiche illecite di violazione dei "segreti commerciali". Il decreto ammette, su richiesta di parte, la possibilità di adottare un percorso alternativo a quello delle misure cautelari, come il pagamento di un indennizzo che deve essere sempre adeguato in rapporto al pregiudizio subito dalla parte che lo ha richiesto. Si prevede l'integrazione dell'art. 388 c.p. con la previsione secondo cui anche chi aggira l'esecuzione di un provvedimento di inibizione o correzione emesso dal giudice a tutela dei diritti di proprietà industriale o chi trasgredisce un provvedimento del giudice con il quale è obbligato a mantenere la riservatezza di informazioni, risponde del delitto di mancata esecuzione dolosa di un provvedimento del giudice. Viene poi riscritto l'art. 623 c.p., che punisce la condotta di chi acquisisce in maniera abusiva segreti commerciali per rivenderli o utilizzarli a proprio o ad altrui vantaggio. La normativa penale aggrava la pena se il fatto è commesso attraverso strumenti informatici, ponendo così un freno alla pericolosa condotta posta in essere da soggetti particolarmente abili con i mezzi informatici.

3 I rapporti con il Parlamento e le altre Istituzioni

3.1. *Le audizioni del Garante in Parlamento*

Nel corso del 2018 il Presidente del Garante ha tenuto alcune audizioni presso Commissioni parlamentari o altri organismi anche bicamerali su temi di interesse all'esame del Parlamento, nell'ambito di indagini conoscitive o nel corso dei lavori per l'approvazione di progetti di legge, segnalandone i riflessi in materia di protezione dei dati personali. In taluni casi è stato chiesto al Garante di trasmettere memorie scritte sugli eventuali profili di criticità delle disposizioni normative in discussione. In questo quadro si collocano, in particolare, le audizioni tenutesi:

– il 7 giugno 2018 (doc. web n. 9003454) presso le Commissioni speciali su atti urgenti del Governo del Senato e della Camera, in seduta congiunta, sullo schema di decreto legislativo per l'adeguamento della normativa nazionale in materia di protezione dati al RGPD (A.G. 22), sul quale si veda *amplius* il par. 2.1;

– il 18 settembre 2018 (doc. web n. 9043373) presso la 11ª Commissione lavoro pubblico e privato, previdenza sociale del Senato su un affare riguardante l'utilizzo di metodologie di *data mining* per eseguire visite mediche di controllo nei confronti dei lavoratori del settore pubblico (Affare n. 58);

– il 2 ottobre 2018 (doc. web n. 9046262) presso le Commissioni riunite I affari costituzionali e XI lavoro della Camera nell'ambito di una proposta di legge recante misure per prevenire e contrastare condotte di maltrattamento o di abuso, anche di natura psicologica, in danno dei minori negli asili nido e nelle scuole dell'infanzia e delle persone ospitate nelle strutture socio-sanitarie e socio-assistenziali per anziani e persone con disabilità (A.C. 1066);

– il 10 ottobre 2018 (doc. web n. 9049788) presso le Commissioni riunite I affari costituzionali e II giustizia della Camera sul tema della trasparenza dei partiti e movimenti politici, nell'ambito dell'esame del pertinente disegno di legge, poi approvato come legge 9 gennaio 2019, n. 3 (cfr. par. 2.3);

– il 27 novembre 2018 (doc. web n. 9064421) presso la 11ª Commissione lavoro pubblico e privato, previdenza sociale del Senato sulle problematiche legate all'utilizzo di sistemi di videosorveglianza e di rilevazione di dati biometrici per il controllo degli accessi al luogo di lavoro, nell'ambito dell'esame del disegno di legge del Governo recante misure per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo (A.S. 920).

In altri due casi il Garante ha inviato alle competenti Commissioni una memoria scritta contenente osservazioni, in particolare:

a) in materia di trasparenza dei rapporti tra le imprese produttrici, i soggetti che operano nel settore della salute e le organizzazioni sanitarie, trasmessa il 5 novembre 2018 (doc. web n. 9065250) alla Commissione Affari sociali della Camera nel corso dell'esame della pertinente proposta di legge (A.C. 491);

b) in materia di Rete nazionale registri tumori, trasmessa il 15 ottobre 2018 (doc. web n. 9065528) alla Commissione igiene e sanità del Senato nel corso dell'esame dei pertinenti disegni di legge (A.S. 535 e abbinati).

3.2. *Le attività di sindacato ispettivo e di indirizzo e controllo del Parlamento*

L'Autorità ha curato il monitoraggio degli atti di sindacato ispettivo e di indirizzo del Parlamento riguardanti possibili aspetti di interesse in materia di protezione dei dati, in relazione ai quali non si segnalano, in questo primo scorcio di legislatura, richieste al Garante di elementi informativi da parte del Governo ai fini della risposta da fornire agli interroganti.

Merita comunque di essere segnalata l'interrogazione n. 5-00911 (on. Bignami e altri) riferita al nuovo sistema di fatturazione elettronica entrato in vigore per tutti i titolari di partita Iva il 1° gennaio 2019 cui è stata fornita risposta dal Governo il 21 novembre. Nel richiamare alcuni profili di criticità relativi al rischio di violazione della protezione dei dati nelle fatture trasmesse all'Agenzia delle entrate, che riportano anche informazioni di carattere personale o relative a transazioni commerciali anche da parte dei terzi fornitori dei sistemi contabili e gestionali, si chiedeva al Governo di sapere quali iniziative di competenza – di carattere tecnico o normativo – intendesse assumere per evitare che i dati e le informazioni sensibili contenute nelle fatture elettroniche trasmesse all'Agenzia delle entrate potessero essere oggetto di cessione integrale o parziale a terzi. Il Sottosegretario intervenuto ha risposto all'interrogazione evidenziando come l'Agenzia delle entrate avesse da tempo intrapreso un approfondito confronto con tutti gli interessati con l'obiettivo di definire regole tecniche e modalità operative in grado di consentire agli operatori economici di adempiere all'obbligo di fatturazione elettronica, e facendo riferimento anche al provvedimento 15 novembre 2018, n. 481 (doc. web n. 9059949) con il quale sono state evidenziate importanti criticità e al tavolo tecnico attivato fra Agenzia delle entrate e Garante finalizzato ad individuare soluzioni idonee a garantire il rispetto della normativa in materia di protezione dei dati personali (cfr. al riguardo par. 4.5.2).

3.3. *L'attività consultiva del Garante*

Il nuovo quadro normativo europeo prevede il parere obbligatorio della Autorità nazionale di controllo anche in relazione alla normativa di rango primario, includendo quindi le iniziative legislative – sia del Parlamento, che del Governo – aventi impatto sulla protezione dei dati personali nel novero dei provvedimenti per la cui elaborazione è necessario consultare il Garante (art. 36, par. 4, e considerando n. 96, RGPD; art. 28, par. 2, direttiva UE 2016/680; art. 24, comma 2, d.lgs. n. 51/2018).

L'art. 36, par. 4, del RGPD non chiarisce con quali modalità e con che tempistica l'obbligo debba essere assolto, sia da parte del Parlamento che del Governo, limitandosi a prevedere che la consultazione avvenga "durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali". Analoga previsione è contenuta nell'art. 28 della direttiva 2016/280, mentre nessuna indicazione specifica al riguardo si rinviene nell'art. 24, d.lgs. n. 51/2018 che dà attuazione al predetto art. 28 in ordine alla consultazione sugli schemi di provvedimenti adottati per finalità di giustizia o di polizia o nel Codice novellato.

3.3.1. I pareri su norme di rango primario

In conformità all'obbligo previsto dalle richiamate previsioni, la Presidenza del Consiglio dei ministri ha richiesto il parere del Garante su uno schema di disegno di legge di iniziativa del Ministro della pubblica amministrazione recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo". In particolare, per quanto di interesse dell'Autorità, per assicurare

l'efficienza della p.a. e il miglioramento dei servizi nonché al fine di eliminare o comunque ridurre false attestazioni di presenza in servizio, il d.d.l. prevede l'applicazione generalizzata di sistemi di rilevazione delle presenze in servizio basati su sistemi di verifica biometrica dell'identità e apparati di videosorveglianza (art. 2). Nel parere reso, il Garante ha indicato una serie di cautele al fine di assicurare la conformità dei trattamenti ai principi di liceità, proporzionalità e "minimizzazione dei dati" (parere 11 ottobre 2018, n. 464, doc. web n. 9051774).

Una volta approdato il progetto di legge in Parlamento (A.S. 920), la Commissione lavoro pubblico e privato del Senato ha richiesto un'audizione del Garante, tenutasi il 27 novembre (cfr. par. 3.1), nel corso della quale il Presidente dell'Autorità ha ribadito la necessità – già rappresentata al Governo nel parere – di rimodulare la disposizione in modo da assicurarne la proporzionalità rispetto alle finalità perseguite. Occorre infatti considerare che, con l'entrata in vigore del RGPD, il principio di proporzionalità è assurto al ruolo di requisito sostanziale della stessa produzione normativa, fungendo al tempo stesso da "limite" all'opera di bilanciamento posta in essere dal potere legislativo degli Stati membri tra interessi diversi e a volte contrapposti. L'art. 7, par. 3, lett. *b*), del RGPD include, infatti, fra i requisiti imprescindibili del "diritto [...] degli Stati membri" (cioè di una adeguata base giuridica nazionale) quello di essere "proporzionato all'obiettivo legittimo perseguito".

Come si è visto, anche in altre occasioni il Parlamento non ha mancato di richiedere al Garante audizioni informali presso le competenti Commissioni o l'inoltro di una memoria scritta su eventuali profili di criticità delle disposizioni normative in discussione. Ciò è avvenuto nel corso dei lavori su progetti di legge relativi a temi di notevole importanza, che spaziano dall'utilizzo di sistemi di videosorveglianza negli asili nido o in luoghi di cura per finalità di prevenzione di maltrattamenti ai danni di bambini o altre persone vulnerabili, alla trasparenza delle erogazioni ai partiti politici e delle competizioni elettorali, a quelle in favore di operatori sanitari da parte di imprese operanti in campo medico-farmaceutico (cfr. al riguardo par. 3.1), a testimonianza del fatto che, al di là delle forme prescelte, il Parlamento ha dimostrato una forte sensibilità sui temi aventi impatto sul diritto alla protezione dei dati personali, coinvolgendo comunque il Garante nel corso del procedimento legislativo.

Il Governo ha inoltre richiesto il parere su alcuni schemi di decreto legislativo.

In un caso si è trattato dello schema di decreto recante disposizioni per la revisione della disciplina del casellario giudiziale, in attuazione della delega di cui alla legge 23 giugno 2017, n. 103, poi divenuto decreto legislativo 2 ottobre 2018, n. 122 (cfr. par. 2.4). Il decreto adegua la disciplina del casellario alle modifiche intervenute nella materia penale, anche processuale e nel diritto dell'Unione europea in materia di protezione dei dati personali, con l'obiettivo della semplificazione del procedimento e della riduzione degli adempimenti amministrativi. Nel parere reso il Garante ha riconosciuto che il trattamento dei dati effettuato nell'ambito degli adempimenti in materia di casellario è da annoverarsi tra le categorie "speciali" di dati (quelli che secondo la definizione del Codice previgente erano i "dati giudiziari") ed è supportato da adeguata base giuridica. Nondimeno si sono fornite alcune precisazioni volte a perfezionare il testo. Con specifico riferimento al limite temporale di conservazione delle iscrizioni nel casellario giudiziale, non è stata accolta la richiesta del Garante di (continuare a) prevedere la morte quale motivo di cancellazione dell'iscrizione, nel rispetto dei principi di proporzionalità, limitazione delle finalità e non eccedenza (artt. 5, RGPD e 3, d.lgs. n. 51/2018). Il decreto stabilisce invece che l'eliminazione dell'iscrizione venga effettuata decorsi quindici anni dalla morte della persona alla quale si riferiscono (e, comunque, decorsi cento anni dalla sua nascita). È stata invece accolta la richiesta, relativa alle procedure di

consultazione del casellario giudiziale in via telematica, di integrare l'art. 4, comma 10, lett. *l*), dello schema con la previsione della necessità di acquisire il parere del Garante sugli schemi di convenzione tra le amministrazioni interessate e il Ministro della giustizia destinate a selezione l'ambito di consultazione dei dati personali in relazione agli specifici procedimenti di competenza e alle fattispecie di reato pertinenti (parere 13 settembre 2018, n. 452, doc. web n. 9055083).

Il Garante ha reso poi parere su uno schema di decreto legislativo recante attuazione della direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (Pnr) a fini di prevenzione e accertamento dei reati di terrorismo e di reati gravi e disciplina dell'obbligo per i vettori di comunicare i dati relativi alle persone trasportate (poi d.lgs. 21 maggio 2018, n. 53: cfr. par. 2.4). Con il predetto decreto, si è inteso disciplinare un ulteriore strumento nelle attività di prevenzione e di contrasto dei reati di terrorismo e di altri reati gravi ed assorbire la normativa introdotta dalla direttiva 2004/82/CE (direttiva Api) recepita con il decreto legislativo 2 agosto 2007, n. 144, che ha introdotto l'obbligo per i vettori aerei di comunicare, ai competenti uffici di polizia di frontiera, talune informazioni relative alle persone trasportate nel territorio dello Stato (Api). Nel parere reso il Garante ha formulato alcuni rilievi volti a perfezionare il provvedimento per renderlo pienamente conforme ai principi ed alle regole in materia di protezione dei dati personali (parere 22 febbraio 2018, n. 100, doc. web n. 8159625).

Infine il Garante ha espresso il richiesto parere sugli schemi dei due decreti legislativi adottati dal Governo per l'adeguamento della normativa nazionale in materia di protezione di dati al RGPD e per l'attuazione della direttiva UE 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, poi divenuti, rispettivamente, decreto legislativo n. 101/2018 e decreto legislativo 18 maggio 2018, n. 51, in relazione ai quali si veda più diffusamente ai paragrafi 2.1 e 2.2.

3.3.2. I pareri sugli atti regolamentari e amministrativi del Governo

Nel quadro dell'attività consultiva concernente norme regolamentari ed atti amministrativi suscettibili di incidere sulla protezione dei dati personali, il Garante ha reso il parere di competenza su numerosi schemi di decreto o di altri provvedimenti, alla stregua della normativa di riferimento (art. 154, comma 4, del Codice, fino al 24 maggio 2018 e successivamente artt. 36, par. 4, e 57, par. 1, lett. *c*), del RGPD).

Ci si riferisce, in particolare, agli schemi relativi al:

1) d.P.R. recante modifica dell'art. 331, d.P.R. 16 dicembre 1992, n. 495, concernente i certificati medici attestanti l'idoneità psicofisica dei conducenti di veicoli a motore (parere 15 febbraio 2018, n. 78, doc. web n. 8043000);

2) decreto del Mef 14 maggio 2018 recante "Modalità tecniche di invio dei dati e di alimentazione del registro degli operatori compro oro", istituito dall'art. 3, d.lgs. 25 maggio 2017, n. 92 (parere 12 aprile 2018, n. 211, doc. web n. 8576294);

3) decreto del Ministro della giustizia recante disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7, commi 1 e 3, d.lgs. 29 dicembre 2017, n. 216 (parere 12 aprile 2018, n. 212, doc. web n. 8987309);

4) decreto del Ministro dello sviluppo economico e del Ministro dell'ambiente e della tutela del territorio e del mare di concerto con i Ministri dell'interno, della salute e dell'economia e delle finanze ai sensi dell'art. 9, comma 1, d.lgs. 6 febbraio 2007, n. 52, che individua il Gestore del registro nazionale delle sorgenti radioattive

e dei relativi detentori e disciplina le modalità di formazione, trattamento, aggiornamento ed accesso ai dati (parere 9 maggio 2018, n. 272, doc. web n. 8997275);

5) decreto del Ministro dell'interno concernente le modalità di accesso al Ced del Dipartimento della pubblica sicurezza da parte della Polizia municipale riguardante i dati dei documenti di identità rubati/smarriti e dei permessi di soggiorno rilasciati/rinnovati (parere 6 giugno 2018, n. 375, doc. web n. 9022276);

6) decreto del Ministro dell'interno concernente le modalità di accesso al Ced del Dipartimento della pubblica sicurezza da parte della Polizia municipale riguardante i dati dei veicoli rubati e l'aggiornamento dei dati medesimi e dei documenti rubati/smarriti (parere 6 giugno 2018, n. 376, doc. web n. 9022288);

7) decreto del Mef concernente il registro informatizzato dei pegni mobiliari non possessori (parere 21 giugno 2018, n. 389, doc. web n. 9022304);

8) d.P.R. recante modifiche ed integrazioni al d.P.R. 19 febbraio 2014, n. 60 relativo alla disciplina del fondo di rotazione per la solidarietà alle vittime dei reati di tipo mafioso, delle richieste estorsive e dell'usura, a norma dell'art. 14, comma 5, l. 7 luglio 2016, n. 122 (parere 28 giugno 2018, n. 395, doc. web n. 9022494);

9) decreto del Mef recante disposizioni in materia di abilitazione all'assistenza tecnica dinanzi alle Commissioni tributarie (parere 11 luglio 2018, n. 416, doc. web n. 9038247);

10) decreto del Ministro dell'interno recante disposizioni per l'applicazione del decreto legislativo 9 aprile 2008, n. 81, in materia di tutela della salute e della sicurezza nei luoghi di lavoro, nell'ambito della articolazioni centrali e periferiche della polizia di Stato e del Dipartimento dei Vigili del fuoco (parere 19 luglio 2018, n. 423, doc. web n. 9040242);

11) d.P.R. recante la disciplina sull'organizzazione e la dotazione delle risorse umane e strumentali per il funzionamento dell'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata ai sensi dell'art. 113-*bis*, comma 1, lett. *a*), d.lgs. 6 settembre 2011 n. 159 (parere 19 luglio 2018, n. 422, doc. web n. 9027168);

12) provvedimento dell'Organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi recante le specifiche tecniche delle procedure di registrazione, accreditamento e consultazione del registro degli operatori compro oro, in attuazione di quanto previsto dall'art. 6 del decreto del Mef 14 maggio 2018, recante le modalità tecniche di invio dei dati e di alimentazione del registro degli operatori compro oro (parere 26 luglio 2018, n. 447, doc. web n. 9025512);

13) decreto del Ministro della giustizia recante il regolamento sulla disciplina dei criteri per l'acquisizione dei dati e delle informazioni rilevanti per individuare i beni giacenti o vacanti nel territorio dello Stato (parere 20 settembre 2018, n. 454, doc. web n. 9054369);

14) d.P.C.M. concernente ulteriori modifiche al decreto 15 settembre 2016, n. 187, recante i criteri e le modalità di attribuzione e di utilizzo della carta elettronica prevista dall'art. 1, comma 979, della legge 28 dicembre 2015, n. 208 e successive modificazioni (*bonus* cultura ai diciottenni), poi divenuto decreto 7 dicembre 2018, n. 138 (parere 07 novembre 2018, n. 477, doc. web n. 9058972).

Ad essi vanno aggiunti ulteriori pareri resi dall'Autorità, rispetto ai quali si richiamano di seguito i luoghi della presente Relazione nei quali agli stessi si fa riferimento. Si tratta del:

15) parere al Mef sulla trasmissione dei dati relativi alle erogazioni liberali, per l'inclusione dei dati nella dichiarazione dei redditi precompilata (parere 11 gennaio 2018, n. 1, doc. web n. 7936278) (cfr. par. 4.5.1);

16) parere al Mef sulla trasmissione dei dati relativi alle rette per la frequenza

degli asili nido, per l'inclusione dei dati nella dichiarazione dei redditi precompilata (parere 11 gennaio 2018, n. 2, doc. web n. 7925253) (cfr. par. 4.5.1);

17) parere su quattro schemi di provvedimento del direttore dell'Agenzia delle entrate attuativi della cd. dichiarazione precompilata (parere 1° febbraio 2018, n. 44, doc. web n. 7772512) (cfr. par. 4.5.1);

18) parere sullo schema di provvedimento del direttore dell'Agenzia delle entrate attuativo della cd. dichiarazione precompilata (parere 8 febbraio 2018, n. 66, doc. web n. 7772714) (cfr. par. 4.5.1);

19) parere sullo schema di decreto del Mef – Ragioniere generale dello Stato attuativo della dichiarazione precompilata (parere 26 aprile 2018, n. 248, doc. web n. 8641178) (cfr. par. 4.5.1);

20) parere al Ministero dell'interno sulle procedure per l'accreditamento al *database* nazionale degli operatori della sicurezza privata (parere 11 luglio 2018, n. 415, doc. web n. 9054325) (cfr. par. 7.2);

21) parere sullo schema di decreto del Ministro della salute relativo all'istituzione e al funzionamento dell'Anagrafe nazionale vaccini (parere 26 luglio 2018, n. 438, doc. web n. 9025504) (cfr. par. 5.2);

22) parere sullo schema di decreto del Mef, di concerto con il Ministero della salute, sulle modalità tecniche e i servizi resi dall'infrastruttura per l'interoperabilità del Fascicolo sanitario elettronico (Fse) (parere 27 settembre 2018, n. 456, doc. web n. 9054337) (cfr. par. 5.1.2);

23) parere al Ministero dell'interno sullo schema di decreto recante modifiche al d.m. 23 dicembre 2015, in materia di modalità tecniche di emissione della carta d'identità elettronica (parere 31 ottobre 2018, n. 476, doc. web n. 9058965) (cfr. par. 4.3.1).

3.4. *L'esame delle leggi regionali*

È proseguita anche nel 2018 l'attività di esame da parte del Garante delle leggi regionali approvate e sottoposte al vaglio di costituzionalità del Governo ai sensi dell'art. 127 della Costituzione, al fine di fornire alla Presidenza del Consiglio dei ministri eventuali elementi di valutazione circa la compatibilità di esse con le disposizioni in materia di protezione dei dati personali e con il dettato costituzionale (art. 117, comma 2, lett, *l*), Cost.).

L'Autorità ha esaminato nel corso dell'anno quattro leggi regionali, ma solo in un caso è stato ritenuto necessario segnalare alla Presidenza del Consiglio dei ministri possibili profili di non conformità al quadro normativo in materia di protezione dati, e precisamente in relazione alla legge della Regione Sardegna 20 marzo 2018, n. 10 recante "Disciplina dell'Anagrafe regionale degli studenti" (nota 11 maggio 2018).

I profili di possibile incostituzionalità si sono riscontrati in relazione alla potestà legislativa esclusiva dello Stato nelle materie della protezione dei dati personali e nella definizione delle norme generali del coordinamento informativo statistico e informatico dei dati. In particolare, il Garante ha rilevato che l'istituzione, da parte della Regione, di una propria Anagrafe regionale degli studenti (Ars) (art. 1) comporta una duplicazione di banche dati, consentendo la raccolta presso la predetta Anagrafe delle medesime informazioni già censite presso l'Anagrafe nazionale degli studenti. Ciò, in contrasto con il divieto previsto dagli artt. 11 del Codice (all'epoca vigente) e 5, par. 1, lett. *c*), del RGPD. Criticità sono state rilevate anche con riferimento alla norma che ha previsto "l'interoperabilità e il collegamento dell'Anagrafe regionale con altri sistemi informativi, banche dati o archivi informatici" (art. 4). La legge regionale non è stata impugnata dal Governo.

L'attività svolta dal Garante

II - L'attività svolta dal Garante

4 Il Garante e le amministrazioni pubbliche

4.1. *I trattamenti di dati sensibili e giudiziari presso le amministrazioni pubbliche*

Il Ministero dell'economia e delle finanze ha formulato un quesito al Garante, relativo alla possibilità di dar corso alle richieste con le quali, richiamando l'art. 26, l. n. 383/2000, associazioni private che statutariamente tutelano gli interessi giuridici degli invalidi di guerra e dei relativi familiari superstiti intendono acquisire elenchi generali nominativi degli appartenenti a tali categorie beneficiari di trattamenti pensionistici. Al riguardo, il Ministero ha precisato che i dati contenuti negli elenchi richiesti, ancorché privi di riferimenti ad elementi anamnestici e diagnostici, costituiscono comunque dati sensibili in quanto la qualifica di invalido di guerra appare idonea a rivelare la situazione di chi, per le proprie condizioni di salute, abbia subito una menomazione dell'integrità fisica, psichica o sensoriale; deve argomentarsi negli stessi termini nel caso di trattamento di reversibilità, considerato che il caso tipico è quello dell'orfano maggiorenne che, dichiarato inabile allo svolgimento di qualsiasi proficuo lavoro, abbia titolo a tale provvidenza.

L'Ufficio, richiamando il quadro normativo di riferimento, ed in particolare le regole e le garanzie più elevate previste per i dati sensibili (artt. 20 e 22, d.lgs. n. 196/2003; regolamento di attuazione degli artt. 20, 21 e 181, d.lgs. n. 196/2003, del Mef, d.m. 29 novembre 2007, n. 255; in particolare, scheda n. 14, "Corresponsione di pensioni di guerra dirette, indirette e di reversibilità"), non ha rilevato i presupposti per effettuare la comunicazione dell'elenco nominativo dei pensionati di guerra all'associazione richiedente, non essendo stata individuata una disposizione che prevede tale comunicazione, né nella menzionata scheda n. 14, né essendosi ritenuta pertinente la base giuridica prospettata dall'associazione richiedente (art. 26, l. n. 383/2000, peraltro abrogato dall'art. 102, comma 1, lett. *a*), d.lgs. n. 117/2017).

In questo senso è stata altresì richiamata una precedente pronuncia dell'Autorità (parere ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013: provv. 10 aprile 2017, n. 188, doc. web n. 6383249) con la quale era stato ritenuto conforme alla disciplina in materia di protezione dei dati personali il diniego opposto dal predetto Ministero ad una istanza di accesso civico presentata dal presidente di un'associazione di invalidi per servizio, avente ad oggetto la "copia dell'elenco dei nominativi, con i relativi indirizzi, dei beneficiari di pensione privilegiata tabellare di cui all'art. 676, d.P.R. 29 dicembre 1973, n. 1092" (nota 17 maggio 2018).

4.2. *La trasparenza amministrativa*

4.2.1. L'accesso civico

L'area di interferenza tra il diritto di accesso civico e la protezione dei dati perso-

nali ha visto l'adozione da parte del Garante, sulla scorta della previsione contenuta nell'art. 5, commi 7 e 8, d.lgs. n. 33/2013, di numerosi pareri resi ai Responsabili della prevenzione della corruzione (Rpct) o ai difensori civici. Anche se le tematiche trattate sono di varia natura, un picco di richieste è stato registrato con riguardo ad accessi civici a dati personali riferiti a lavoratori e dipendenti della p.a.; quindi, a dati personali contenuti in titoli abilitativi edilizi, a sentenze, atti e dati giudiziari, a tasse e contributi, a verbali della polizia municipale nonché a permessi per veicoli (concessione spazi di sosta per disabili, transito e sosta nelle Ztl). Alla fattispecie più significative, suddivise per aree tematiche, si dà sinteticamente conto nelle pagine a seguire.

Dimissioni

Il Garante è intervenuto in relazione al caso della presentazione di un'istanza di accesso civico generalizzato all'atto con il quale un dipendente comunale aveva rassegnato le proprie dimissioni, ritenendo corretto il rifiuto dell'amministrazione. Ciò in quanto i documenti richiesti contenevano dati e informazioni personali (oltre al nominativo e all'incarico ricoperto dal dipendente, anche la descrizione dei motivi di carattere strettamente personale che lo avevano indotto a rassegnare le dimissioni), con la conseguenza che la relativa ostensione poteva causare un pregiudizio concreto alla protezione dei dati personali dell'interessato. Nel caso esaminato, peraltro, non era possibile accordare neanche un accesso parziale ai documenti in questione, in quanto l'eventuale oscuramento del nominativo dell'interessato non avrebbe eliminato completamente la possibilità di sua re-identificazione, anche da parte di terzi, alla luce della complessiva vicenda descritta e delle ulteriori informazioni contenute nel documento di cui è stata negata l'ostensione (parere 15 febbraio 2018, n. 75, doc. web n. 8125663).

Progressioni economiche orizzontali

Il Garante ha avuto occasione di pronunciarsi anche in relazione all'accesso civico a graduatorie per le progressioni economiche orizzontali di dipendenti di una Camera di commercio recanti i punteggi attribuiti. Nel caso di specie, l'ente aveva accolto parzialmente la richiesta di accesso civico autorizzando la trasmissione del documento, oscurando però i nominativi (nonché gli eventuali altri elementi di identificazione, anche indiretta) degli interessati. A fronte della richiesta di riesame volta ottenere l'ostensione integrale del documento, è stata ritenuta la conformità delle modalità con cui la Camera di commercio aveva accordato l'accesso civico parziale alla graduatoria richiesta rispetto alla disciplina in materia di protezione dei dati, in quanto le informazioni personali ivi contenute erano state oscurate. Il riconoscimento di un eventuale accesso civico ai dati personali dei dipendenti contenuti nella citata graduatoria, infatti, unita alla generale conoscenza e al particolare regime di pubblicità dei dati oggetto di accesso civico, avrebbe potuto arrecare agli interessati, a seconda delle ipotesi e del contesto in cui i dati e le informazioni fornite possono essere utilizzate da terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013. Ciò tenendo conto anche di quanto evidenziato dall'amministrazione, secondo la quale un eventuale accesso ai dati personali richiesti, poiché riferiti ai singoli dipendenti, poteva esporli a difficoltà relazionali con i colleghi di lavoro e creare ingiustificati pregiudizi da parte degli utenti esterni che venissero a contatto con gli stessi nell'esercizio delle loro funzioni (parere 8 marzo 2018, n. 142, doc. web n. 8684742).

In un altro caso, il Garante ha concordato con la decisione di un Consiglio regionale con la quale era stata respinta la richiesta di accesso alla documentazione funzionale all'approvazione di una graduatoria per la progressione economica del proprio personale (parere 18 aprile 2018, n. 231, doc. web n. 8983308). Ciò considerando la tipologia e la natura dei dati e delle informazioni personali oggetto dell'i-

stanza di accesso civico nel caso in esame, attinenti peraltro anche a profili di dettaglio della vita lavorativa e della moralità di dipendenti pubblici partecipanti alla selezione interna all'amministrazione finalizzata alla progressione della categoria economica, la cui ostensione poteva comportare ripercussioni negative per gli interessati, anche sul piano relazionale e professionale, sia all'interno dell'ambiente lavorativo che all'esterno (ad es., per prospettive di impiego cui gli interessati potrebbero aspirare al di fuori dell'amministrazione, oppure per la possibile esposizione a condotte censurabili quali minacce, intimidazioni, ritorsioni o turbative al regolare svolgimento delle funzioni pubbliche o delle attività di pubblico interesse esercitate). Inoltre, è stato ritenuto che il medesimo Consiglio aveva correttamente respinto anche un eventuale accesso civico parziale a documenti richiesti con oscuramento dei dati personali, in quanto, dal complesso delle informazioni e delle vicende ivi riportate, gli interessati avrebbero potuto essere facilmente re-identificati, anche da terzi operanti nella medesima amministrazione.

Il Garante è intervenuto con un parere su un accesso civico concernente un'ampia documentazione relativa ad una selezione per l'attribuzione della progressione economica orizzontale per il personale di una Giunta regionale, contenente dati e informazioni personali di varia specie e natura, che – oltre a riguardare dati identificativi, di residenza e di contatto – afferivano alla posizione giuridica ed economica dei dipendenti, agli aspetti della vita lavorativa e alla qualità delle prestazioni svolte, alla formazione e all'aggiornamento professionale (parere 11 ottobre 2018, n. 466, doc. web n. 9063969). In tale circostanza è stato evidenziato che non era possibile accordare una generale prevalenza al diritto di accesso generalizzato a scapito di altri diritti ugualmente riconosciuti dall'ordinamento (quali, ad es., quello alla riservatezza e alla protezione dei dati personali). Ciò in quanto si sarebbe vanificato il necessario bilanciamento degli interessi in gioco che richiede un approccio equilibrato nella ponderazione dei diversi diritti coinvolti, tale da evitare che i diritti fondamentali di eventuali controinteressati possano essere gravemente pregiudicati dalla messa a disposizione a terzi – non adeguatamente ponderata – di dati, informazioni e documenti che li riguardano. Nel caso di specie è stato ritenuto quindi corretto il rifiuto opposto dall'amministrazione all'accesso civico, in quanto, considerata la tipologia e la natura dei dati e delle informazioni personali richiesti, la relativa ostensione poteva determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei controinteressati, potendoli esporre a difficoltà relazionali con i colleghi di lavoro e creare ingiustificati pregiudizi da parte degli utenti esterni che potevano venire in contatto con gli stessi nell'esercizio delle loro funzioni, con conseguenti ripercussioni negative sul piano professionale, personale, sociale e relazionale, sia all'interno che all'esterno dell'ambiente lavorativo. La presenza nella documentazione richiesta di dati e informazioni dettagliati dei controinteressati rendeva inoltre particolarmente difficile, se non impossibile, l'anonimizzazione dei documenti, con la conseguenza di impedire anche un eventuale accesso civico parziale ai sensi dell'art. 5-*bis*, comma 4, d.lgs. n. 33/2013.

Accesso alla qualifica dirigenziale

In un'altra occasione – concernente l'accesso civico a documentazione inerente l'accesso alla qualifica dirigenziale –, a fronte del diniego opposto dall'amministrazione, è stato osservato che quest'ultima non può sottrarsi, per motivi inerenti alla protezione dei dati personali, all'accoglimento della richiesta relativamente al bando di concorso pubblico, per titoli ed esami, per dirigenti e alla relativa graduatoria (entrambi pubblicati in G.U.). Sono stati invece ritenuti non accessibili i documenti, quali il certificato di laurea e la certificazione dell'anzianità di servizio con indicazione della data di inquadramento del livello giuridico del dipendente, la cui ostensione, unita alla generale conoscenza e al particolare regime di pubblicità del-

4

l'accesso civico generalizzato, era in grado di provocare all'interessato un pregiudizio concreto alla tutela della protezione dei dati personali (parere 18 gennaio 2018, n. 26, doc. web n. 7688820; cfr. anche parere 8 marzo 2018, n. 143, doc. web n. 8357482).

In tema di accesso alla qualifica dirigenziale, ribadendo quanto precedentemente affermato, è stato evidenziato come, in altra fattispecie, dovessero essere considerati non accessibili documenti, quali i contratti di lavoro, contenendo gli stessi dati la cui ostensione avrebbe potuto procurare ripercussioni negative, soprattutto sul piano relazionale e professionale, al controinteressato. Ciò anche considerando la ragionevole aspettativa di confidenzialità del dirigente riguardo alle informazioni detenute dall'ente presso il quale prestava servizio, inerenti ai rapporti contrattuali instaurati anche con precedenti datori di lavoro; nonché la non prevedibilità da parte dello stesso delle conseguenze derivanti dalla conoscibilità da parte di chiunque dei predetti dati e informazioni richiesti tramite l'accesso civico (parere 18 aprile 2018, n. 230, doc. web n. 8987117).

Informazioni su incarichi esterni

In tema di accesso civico ai dati riferiti ai dipendenti, è stato approvato un articolato parere relativo agli incarichi esterni dagli stessi rivestiti (parere 29 marzo 2018, n. 179, doc. web n. 8685129). Al riguardo, è stato rappresentato che – fermi restando gli obblighi di pubblicazione di cui all'art. 18, d.lgs. n. 33/2013 – la mancata ostensione di alcuni documenti non risultava motivata nel provvedimento di diniego della p.a. e in ogni caso, nel caso esaminato, per alcuni degli atti richiesti non era comunque richiamabile il limite all'accesso civico previsto dall'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013, considerando la natura dei dati personali ivi contenuti (peraltro già resi pubblici in atti di sindacato ispettivo presso gli organi parlamentari e da quotidiani nazionali), il ruolo ricoperto dal controinteressato nella vita pubblica, la connessa funzione pubblica esercitata e l'attività di pubblico interesse svolta nel periodo, seppur breve, in cui era stato assunto un incarico istituzionale presso un ente locale. In ordine alla restante documentazione – inerente agli incarichi esterni svolti a titolo personale (art. 53, comma 6, d.lgs. 20 marzo 2001, n. 165) – è stato affermato che, in linea di principio, una generale richiesta di accesso civico a tutti gli incarichi svolti durante l'intera vita lavorativa di un dipendente presso una p.a. può consentire la conoscenza di informazioni attraverso le quali ricostruire l'attività svolta "a titolo personale" e al di fuori dell'orario di lavoro da parte di un dipendente. Inoltre, nel caso di specie l'istanza di accesso civico non precisava né il periodo temporale, né la categoria di documenti cui si desiderava accedere e l'amministrazione, nel provvedimento di riscontro dell'accesso civico, non aveva descritto le ragioni per le quali l'ostensione dei documenti richiesti poteva comportare un pregiudizio concreto alla protezione dei dati personali dell'interessato. Tali circostanze non hanno permesso quindi di esprimere un parere nel merito della questione sottoposta, sì che la p.a. istante è stata invitata a rivalutare la richiesta di accesso, fornendo nella risposta una motivazione congrua e completa rispetto all'esistenza o meno del limite di cui all'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013. Ciò tenendo conto delle motivazioni del controinteressato e della circostanza che fra lo stesso e l'istante pendeva un contenzioso giudiziario; della circostanza che alcune informazioni erano già di pubblico dominio (ad es., partecipazione a convegni e seminari pubblici soprattutto se recenti); del fatto che la documentazione richiesta riguardava l'intera vita lavorativa del controinteressato e quindi l'ostensione dei documenti richiesti, se non circoscritta a un determinato periodo di tempo, poteva risultare sproporzionata rispetto allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico.

Con riferimento allo svolgimento di incarichi esterni, è stata esaminata un'istanza di riesame (presentata dai controinteressati) di un provvedimento di accoglimento di un accesso civico avente ad oggetto la copia delle autorizzazioni degli incarichi esterni svolti da due professori universitari (parere 31 maggio 2018, n. 373, doc. web n. 9001960). L'amministrazione è stata invitata a rivalutare il provvedimento di accoglimento integrale dell'accesso civico, verificando la possibilità di accordarlo solo in forma parziale, limitandolo ai soli documenti contenenti la richiesta dei professori recante in calce l'autorizzazione dell'Università allo svolgimento dell'incarico extraistituzionale ed oscurando i dati non oggetto di pubblicazione obbligatoria ai sensi della disciplina di trasparenza (art. 18, d.lgs. n. 33/2013), non necessari ai sensi dell'art. 5, par. 1, lett. *c*), del RGPD (ad es., il codice fiscale). Si è concordato, invece, con il diniego all'accesso civico alla copia dei contratti allegati a detta autorizzazione poiché tale ostensione, come evidenziato dall'amministrazione, sarebbe risultata sproporzionata rispetto allo scopo dell'istituto, essendo eccedenti le informazioni di dettaglio contenute nella documentazione, comprensive anche di dati personali, la cui conoscenza (e successiva eventuale divulgazione) da parte del richiedente avrebbe potuto arrecare un pregiudizio concreto ai controinteressati, contravvenendo così alle prescrizioni dell'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013.

Valutazione della *performance*

A fronte di un'istanza di accesso concernente la documentazione riguardante le valutazioni di tutto il personale di polizia municipale in tre anni (dal 2014 al 2016), è stato ritenuto che il comune aveva correttamente respinto la richiesta, poiché l'ostensione dei dati e delle informazioni richieste avrebbe potuto determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei controinteressati, con ripercussioni negative sul piano professionale, personale, sociale e relazionale, sia all'interno che all'esterno dell'ambiente lavorativo (parere 11 luglio 2018, n. 421, doc. web n. 9037343). Inoltre, è stato evidenziato che la presenza nei verbali di valutazione delle *performance* del personale dipendente di dati e informazioni dettagliati dei controinteressati avrebbe reso particolarmente difficile, se non impossibile, l'anonimizzazione dei documenti, con la conseguenza di impedire anche un eventuale accesso civico parziale ai sensi dell'art. 5-*bis*, comma 4, d.lgs. n. 33/2013. Nessun ostacolo invece si sarebbe potuto porre per l'ostensione delle informazioni relative alle modalità generali di valutazione delle *performance* individuali (ad es., quelle relative ai criteri di misurazione), tenuto conto che, in base alla disciplina sulla trasparenza amministrativa, tali informazioni sono oggetto di pubblicazione obbligatoria (artt. 10, comma 8, lett. *b*), e 20, d.lgs. n. 33/2013).

Presenze e assenze in servizio, compenso percepito e straordinari

In relazione alla richiesta di dati personali dei lavoratori, è stato ritenuto corretto il rifiuto del Mef all'accesso civico avente a oggetto le presenze e gli straordinari di propri dipendenti, poiché la predetta documentazione, anche se epurata dai dati inerenti alle assenze per malattia, conteneva in ogni caso un'estesa gamma di dati e informazioni, particolarmente delicati, anche considerando il lungo arco temporale – dai due ai quattro anni, a seconda dei dipendenti – a cui erano riferiti. È stato inoltre evidenziato che per i fogli di presenza dei lavoratori non è previsto alcun tipo di regime di pubblicità e non è possibile considerarli come atti pubblici come sostenuto, invece, dall'istante (parere 27 settembre 2018, n. 458, doc. web n. 9049940).

In un altro caso è stata confermata la validità del diniego opposto da una società a totale partecipazione pubblica a una istanza di accesso civico generalizzato avente ad oggetto alcuni documenti contenenti dati e informazioni personali riferiti a lavoratori a termine, quali presenze e assenze in servizio, nonché al compenso percepito per il periodo di impiego. L'ostensione di quanto richiesto, unita al particolare regime di pubblicità dei dati oggetto di accesso civico, poteva infatti arrecare ai

dipendenti, a seconda delle ipotesi e del possibile utilizzo da parte di terzi, un pregiudizio concreto alla tutela dei dati personali come previsto dall'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013. È stato inoltre aggiunto che la generale conoscenza delle predette informazioni personali poteva determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei controinteressati, con possibili ripercussioni negative sul piano professionale, personale, relazionale e sociale. Ciò anche tenendo conto delle ragionevoli aspettative di confidenzialità in relazione al trattamento dei dati personali al momento in cui questi erano stati raccolti dalla società, nonché della non prevedibilità, al momento della raccolta, delle conseguenze derivanti dalla eventuale conoscibilità da parte di chiunque dei dati oggetto di richiesta (parere 19 dicembre 2018, n. 516, doc. web n. 9075337).

Trattamento giuridico ed economico del personale

Il Garante ha reso un parere nel caso di una richiesta di riesame avverso il silenzio dell'amministrazione, che non aveva fornito alcun riscontro ad un'istanza di accesso civico generalizzato volta a conoscere una serie di documenti riguardanti un proprio dipendente, tra i quali la domanda di partecipazione ad una selezione e l'inquadramento giuridico ed economico. In tale caso, dopo aver osservato, in via preliminare, che l'amministrazione non aveva espressamente negato o differito l'accesso per motivi attinenti alla tutela dei dati personali, limitandosi a comunicare all'istante che il controinteressato aveva presentato opposizione all'ostensione, è stato osservato che tale riscontro risultava essere eccessivamente sintetico e non consentiva di comprendere appieno quali fossero state in concreto le ragioni del diniego all'ostensione dei documenti richiesti. Tuttavia, pur non potendosi il Garante pronunciare nel merito della questione per ragioni di competenza, è stato evidenziato che in relazione ai dati e alle informazioni riferiti al dipendente e relativi all'attività lavorativa (inquadramento giuridico ed economico, retribuzione lorda annua, retribuzione di risultato, rimborsi per spese di missione) nonché alla procedura di selezione cui aveva partecipato, esistevano precedenti pareri resi su casi analoghi nei quali l'Autorità aveva evidenziato la possibilità che l'ostensione dei predetti documenti poteva in ogni caso arrecare al controinteressato un concreto e reale pregiudizio alla tutela dei propri dati personali, con possibili ripercussioni negative sul piano professionale, personale e sociale (parere 29 novembre 2018, n. 485, doc. web n. 9065367).

Condono edilizio e concessione in sanatoria

In relazione all'istanza di accesso civico avente ad oggetto un'articolata documentazione relativa a una procedura di condono edilizio, è stata condivisa la posizione dell'amministrazione che ha negato l'accesso, reputando prevalente la tutela delle numerose informazioni personali contenute negli atti richiesti. Nel caso di specie, peraltro, si trattava di documenti presentati da oltre un trentennio e relativi a una procedura ormai conclusa, con la conseguenza che l'ostensione e la diffusione generale di questi ultimi poteva arrecare, anche agli eredi (in qualità di controinteressati), un pregiudizio concreto alla tutela degli interessi protetti dall'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (parere 18 gennaio 2018, n. 25, doc. web n. 7688896).

Con riguardo all'accesso civico a copiosa documentazione riguardante una procedura di condono edilizio (copia della domanda, documenti integrativi, concessione edilizia in sanatoria, etc.), contenente dati e informazioni personali di diversa specie e natura, è stato ritenuto che l'amministrazione avesse correttamente rigettato l'istanza ai sensi dell'art. 5-*bis,* comma 1, lett. *a*), d.lgs. n. 33/2013, poiché l'ostensione dei dati e delle informazioni richieste poteva determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà del controinteressato, con ripercussioni negative sul piano sociale, relazionale e professionale. Ciò anche tenendo conto delle ragionevoli aspettative di confidenzialità dell'interessato in relazione al

trattamento dei propri dati personali al momento in cui questi sono stati raccolti dal Comune, nonché alla non prevedibilità, al momento della raccolta dei dati, delle conseguenze derivanti a quest'ultimo dalla eventuale conoscibilità da parte di chiunque dei dati oggetto di richiesta (parere 3 maggio 2018, n. 260, doc. web n. 8997418).

Il Garante non si è pronunciato sul caso inerente una richiesta di accesso civico alla copia della concessione edilizia e dell'eventuale concessione in sanatoria di un immobile, poiché dagli atti non risultava comprensibile se i dati e le informazioni contenuti nella documentazione richiesta fossero riferibili a persone fisiche o giuridiche. In quest'ultima ipotesi, infatti, la disciplina in materia di protezione dei dati personali non è applicabile, considerando che sono dati personali solo quelli riferibili a persone fisiche (parere 22 febbraio 2018, n. 103, doc. web n. 8357130).

Permesso di costruire

È stato ritenuto giustificato il diniego opposto a una richiesta di accesso civico generalizzato a permessi di costruire e alla relativa documentazione, in quanto l'istanza investiva, oltre ai dati oggetto di un preciso regime di pubblicità (art. 20, d.P.R. n. 380/2001), anche ulteriore (ampia) documentazione relativa all'istruttoria degli atti, contenenti dati e informazioni personali di diversa specie e natura (titoli di proprietà, ai nominativi, data e luogo di nascita, codici fiscali, residenza, e-mail, Pec, numeri di telefono, dei titolari dell'intervento o dei loro rappresentanti, dati dei tecnici incaricati, informazioni sulla tipologia di intervento, ubicazione, dati catastali e destinazione d'uso dell'immobile, dichiarazioni concernenti il versamento degli oneri nonché elaborati progettuali). La potenziale diffusione di tali informazioni, alla luce dell'amplificato regime di pubblicità dell'accesso civico, avrebbe infatti potuto causare un pregiudizio concreto alla protezione dei dati personali dei controinteressati. Ciò anche considerando le ragionevoli aspettative di riservatezza di questi ultimi circa il trattamento dei propri dati personali al momento in cui questi sono stati raccolti dall'amministrazione. È stata condivisa inoltre la considerazione dell'amministrazione secondo cui sarebbe stato impossibile concedere un accesso civico parziale in quanto, anche oscurando i dati del committente, l'indicazione dell'immobile oggetto di intervento avrebbe consentito di risalire all'identità del proprietario tramite visure catastali (parere 8 febbraio 2018, n. 68, doc. web n. 8052934).

Certificati e concessioni edilizie

In relazione alla richiesta di accesso civico a certificati edilizi, è stato evidenziato che i titoli edilizi possono contenere dati e informazioni personali della natura più varia, quali dati identificativi e anagrafici dei richiedenti (se persone fisiche), dei loro rappresentanti e dei tecnici progettisti, la titolarità dell'immobile, l'indicazione dei dati catastali, nonché informazioni sui pareri acquisiti da altri organismi oltre che relativi all'opera da costruire. Agli stessi documenti sono inoltre di norma allegati atti contenenti informazioni puntuali sulla tipologia di intervento o sulla destinazione d'uso dell'immobile oggetto del permesso, gli elaborati progettuali, etc. Nel caso di specie, tuttavia, dagli atti dell'istruttoria non è emersa la sicura riferibilità dei dati contenuti nella documentazione richiesta a persone fisiche o giuridiche e ciò ha impedito la possibilità di entrare nel merito della questione, considerando che laddove gli atti richiesti fossero riconducibili a enti o persone giuridiche, la disciplina di protezione dei dati personali non avrebbe potuto trovare applicazione, essendo il concetto di dato personale, come ricordato in precedenza, riferibile esclusivamente alle persone fisiche (parere 22 maggio 2018, n. 359, doc. web n. 9001943).

In un altro caso è stato ritenuto fondato il rigetto di un'istanza di accesso civico riguardante una concessione edilizia contenente dati e informazioni personali del controinteressato, poiché la relativa ostensione, unita peraltro al particolare regime

di pubblicità dei dati oggetto di accesso civico, avrebbe potuto determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dello stesso, con ripercussioni negative sul piano personale, sociale e relazionale. Ciò anche tenendo conto dei rapporti intercorrenti tra il controinteressato e l'istante, tra i quali risultava pendente un procedimento penale (parere 5 luglio 2018, n. 410, doc. web n. 9037331).

Scia e Cila

Il Garante è intervenuto in un caso inerente una richiesta di accesso civico generalizzato alla documentazione relativa alle segnalazioni certificate di inizio attività (Scia) e alle comunicazioni di inizio attività asseverata (Cila), identico a quello per il quale era stato reso il precedente parere del 10 agosto 2017, n. 360 (doc. web n. 6969290) al quale pertanto è stato fatto rinvio (provv. 19 dicembre 2018, n. 517, doc. web n. 9073695). Tuttavia, rispetto all'eccezione del richiedente secondo cui nel precedente parere non si sarebbe sufficientemente "specificato" in ordine al "pregiudizio concreto alla tutela della protezione dei dati personali, posto fra i motivi alla base del diniego", è stato evidenziato – anche per dare conto dell'intervenuta applicazione dal 25 maggio 2018 del RGPD – che il trattamento dei dati personali deve avvenire nel rispetto del principio di minimizzazione, secondo il quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 4, par. 1, n. 1; art. 5, par. 1, lett. *c*), del RGPD). A ciò si aggiunga che i dati e i documenti ricevuti a seguito di una istanza di accesso civico divengono "pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli" ai sensi dell'art. 7, d.lgs. n. 33/2013. Pertanto, è anche alla luce di tale amplificato regime di pubblicità che va valutata l'esistenza di un possibile pregiudizio concreto. Nel caso esaminato è stato quindi reputato che la generale conoscenza delle informazioni personali contenute nelle Scia e nelle Cila poteva determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei controinteressati – in violazione del principio di minimizzazione dei dati sopra richiamato – con possibili ripercussioni negative sul piano professionale, personale e sociale. Ciò anche tenendo conto delle ragionevoli aspettative di confidenzialità dei controinteressati in relazione al trattamento dei propri dati personali al momento in cui questi sono stati raccolti dall'amministrazione, nonché della non prevedibilità, al momento della raccolta, delle conseguenze derivanti dalla eventuale conoscibilità da parte di chiunque dei dati richiesti tramite l'accesso civico (sul punto cfr. anche il più recente parere reso sulla medesima questione del 3 gennaio 2019, n. 1, doc. web n. 9080951).

In altro caso, inerente un provvedimento di accesso civico alla documentazione relativa alle Scia e alle Cila presentate in un dato territorio e con un determinato orizzonte temporale, considerando che la fattispecie era identica – in relazione sia all'oggetto sia al soggetto richiedente – a quella per la quale è stato reso il parere n. 360 del 10 agosto 2017, si è concordato con il diniego opposto dall'amministrazione, rinviando al predetto parere (parere 13 settembre 2018, n. 453, doc. web n. 9050702).

Accertamento di irregolarità edilizie

Il Garante ha inoltre ritenuto corretto il diniego opposto a una istanza di accesso civico generalizzato volta a ottenere una serie di provvedimenti di accertamento di irregolarità edilizie (parere 7 agosto 2018, n. 449, doc. web n. 9044701). In particolare, al di fuori dei documenti soggetti a obbligo di pubblicazione ai sensi del d.P.R. n. 380/2001 e pubblicati oscurando i dati personali, è stato affermato che il comune aveva correttamente negato l'accesso ai restanti atti, in quanto, trattandosi di una vicenda non ancora accertata come illecito penale e/o amministrativo – con un possibile avvio del procedimento penale a carico dei presunti autori degli abusi

– e tenendo conto sia della natura dei dati e delle informazioni personali contenute nella documentazione richiesta, sia del ristretto ambito territoriale del comune interessato, dall'ostensione poteva derivare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei controinteressati, con possibili ripercussioni negative sul piano lavorativo, professionale, personale e sociale.

In relazione al provvedimento di diniego nei confronti di una istanza di accesso civico generalizzato, avente a oggetto la documentazione di un giudizio pendente dinnanzi al Tar, il relativo numero di ruolo, nonché le date delle future udienze, è stato osservato che l'art. 5-*bis*, comma 3, d.lgs. n. 33/2013, annovera nei casi di esclusione "i divieti di accesso o divulgazione previsti dalla legge, ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti". A tal riguardo, gli atti e i documenti inseriti nel fascicolo d'ufficio e delle parti, relativi ai procedimenti giudiziari, restano conoscibili nelle modalità previste alle relative disposizioni processuali – fra cui l'art. 76 delle disposizioni per l'attuazione del c.p.c. e le disposizioni transitorie, che non possono essere derogate dalla disciplina in materia di accesso civico. Ciò anche considerando quanto precisato dall'Anac nelle Linee guida (del. 28 dicembre 2016, n. 1309) ovvero che "esulano dall'accesso generalizzato gli atti giudiziari, cioè gli atti processuali o quelli che siano espressione della funzione giurisdizionale, ancorché non immediatamente collegati a provvedimenti che siano espressione dello *ius dicere*, purché intimamente e strumentalmente connessi a questi ultimi. L'accesso e i limiti alla conoscenza degli atti giudiziari, ovvero di tutti gli atti che sono espressione della funzione giurisdizionale, anche se acquisiti in un procedimento amministrativo, sono disciplinati da regole autonome previste dai rispettivi codici di rito" (parere 25 gennaio 2018, n. 41, doc. web n. 7828631).

Analogamente, il Garante è intervenuto nel caso di un'istanza di accesso civico generalizzato avente ad oggetto: la copia delle sentenze e dei provvedimenti, emessi negli ultimi cinque anni, con cui l'autorità giudiziaria ha condannato al pagamento di somme in favore di un Comune; lo stato attuale di riscossione; gli ulteriori analoghi provvedimenti giudiziari antecedenti i cinque anni, laddove non interamente adempiuti. In tal caso è stato ritenuto conforme alla disciplina in materia di protezione dei dati personali la scelta della p.a. di concedere l'accesso parziale. In particolare, è stato rilasciato un elenco anonimo riportante: il numero di sentenza e l'anno di riferimento, l'autorità giudiziaria, l'oggetto della lite, lo stato attuale dell'azione esecutiva intrapresa dall'amministrazione e l'eventuale riscossione. Negli atti giudiziari, infatti, sono contenute numerose informazioni di carattere personale, quali la qualità di debitore, l'impossibilità di restituire le somme a causa di un Isee basso, l'esistenza di un pignoramento o di un decreto ingiuntivo in corso, la concessione della rateizzazione del pagamento, l'esistenza di vertenze in materia di lavoro, la conclusione di accordi transattivi, la cui ostensione integrale unita al particolare regime di pubblicità dei dati e documenti oggetti di accesso civico, avrebbe potuto determinare un pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (parere 25 gennaio 2018, n. 42, doc. web n. 7810482).

In un'altra circostanza il Garante ha ritenuto corretto il rigetto dell'istanza di accesso avente a oggetto note, rilievi e raccomandazioni dell'Anac – contenenti dati personali e giudiziari inerenti procedimenti penali ancora in corso – posto che si poteva realizzare a carico dei controinteressati un pregiudizio concreto alla tutela della protezione dei dati personali (parere 16 maggio 2018, n. 291, doc. web n. 8997258). L'ostensione dei predetti dati, unita al particolare regime di pubblicità dei dati oggetto di accesso civico, avrebbe determinato infatti un'interferenza ingiu-

stificata e sproporzionata nei diritti e libertà dei controinteressati, nonché ripercussioni negative, anche sul piano relazionale e professionale, sia all'interno che all'esterno dell'ambiente lavorativo. Ciò anche tenendo conto delle ragionevoli aspettative di confidenzialità degli interessati in relazione al trattamento dei propri dati personali al momento in cui questi sono stati raccolti, nonché alla non prevedibilità, al momento della raccolta dei dati, delle conseguenze a essi derivanti dalla eventuale conoscibilità da parte di chiunque dei dati richiesti tramite l'accesso civico. Nel caso di specie inoltre non risultava possibile fornire nemmeno un accesso parziale, in quanto i citati controinteressati risultavano comunque indirettamente identificabili.

Sempre in tema di dati e atti giudiziari il Garante ha reso un parere riguardante una richiesta di riesame di un provvedimento di rifiuto di accesso civico ad una nota comunale, i cui estremi erano contenuti in una deliberazione pubblicata sul sito web, concernente la costituzione di parte civile dello stesso comune in un procedimento penale, alla quale era allegata altresì la richiesta di rinvio a giudizio firmata dal pubblico ministero nei confronti di numerosi soggetti (parere 15 novembre 2018, n. 482, doc. web n. 9063993). Sul punto, dopo aver osservato che in tali documenti erano contenuti dati personali di diversa specie e natura, riferibili oltre che all'autore della nota anche a terzi, nonché informazioni inerenti alla commissione di reati e procedimenti penali attualmente in corso, è stato ritenuto corretto l'operato del comune che ha respinto l'istanza di accesso civico, in quanto tale ostensione poteva arrecare all'autore della nota e agli altri controinteressati un pregiudizio concreto alla tutela della protezione dei dati personali, così come normativamente previsto, con possibili ripercussioni negative sul piano personale e sociale.

In relazione a un contenzioso civile è stato emesso anche un altro parere richiamando in particolare l'attenzione sul fatto che l'ostensione di dati personali, anche alla luce del principio di "minimizzazione" (art. 5, par. 1, lett. *c*), del RGPD), non deve determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà delle persone cui si riferiscono tali dati (parere 20 dicembre 2018, n. 518, doc. web n. 9069884). È stato ricordato altresì che nel riscontrare l'accesso civico bisogna tenere in considerazione la natura dei dati personali richiesti; l'esistenza di una "ragionevole aspettativa" di riservatezza in relazione al momento in cui i dati sono stati raccolti; la prevedibilità, al momento della raccolta, delle conseguenze derivanti dalla eventuale conoscibilità da parte di chiunque dei predetti dati; infine, il ruolo ricoperto nella vita pubblica e l'attività di pubblico interesse svolta dai controinteressati. Ciò anche considerando che, nel caso in esame, i controinteressati erano soggetti che rivestivano o avevano rivestito incarichi di indirizzo politico e alcune delle informazioni richieste sarebbero risultate già di pubblico dominio.

Tasse e canoni

Il Garante è intervenuto anche in relazione a richieste di accesso civico ad atti relativi al pagamento di tasse e contributi erariali. Al riguardo, a fronte di un'istanza di accesso civico concernente la copia autentica in formato cartaceo inerente al pagamento dei tributi (dichiarazioni Imu, Tasi, Tari) dovuti dalle persone fisiche, proprietari di un immobile di cui venivano forniti i dati catastali, è stata condivisa la posizione della p.a. sul fatto che dalla tipologia e dalla natura dei dati e delle informazioni personali richiesta era possibile ricostruire la posizione tributaria dei contribuenti e, di conseguenza, la loro situazione economica personale. Pertanto, si è ritenuto che l'amministrazione aveva correttamente negato l'accesso civico, in quanto l'ostensione della documentazione richiesta poteva comportare ai controinteressati ripercussioni negative, anche sul piano sociale e relazionale, con pregiudizio concreto alla protezione dei dati personali ai sensi dell'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (parere 14 giugno 2018, n. 382, doc. web n. 9001972; cfr. anche parere 30 novembre 2017, n. 506, doc. web n. 7316508).

Analogamente, con riferimento all'accesso civico a documentazione riguardante l'accertamento effettuato da un comune sul versamento dell'Imu su un immobile in comproprietà fra l'istante e altri soggetti, è stato affermato che l'ostensione dei dati ivi contenuti era suscettibile di determinare un pregiudizio concreto alla tutela della protezione dei dati personali. Pertanto è stata evidenziata la necessità che l'amministrazione motivasse specificamente le ragioni dell'esistenza di tale pregiudizio (parere 12 aprile 2018, n. 215, doc. web n. 8790715).

Per altro verso, a fronte di un'istanza di accesso civico generalizzato concernente documenti e informazioni di dettaglio sul pagamento del canone per l'occupazione di spazi ed aree pubbliche, è stato ritenuto che dalla documentazione inviata dall'amministrazione per ricevere il prescritto parere non si poteva comprendere se le predette informazioni fossero riferite a persone fisiche o giuridiche (distinzione rilevante in quanto, come già detto, sono sottratte dall'ambito di applicazione della disciplina in materia di protezione dei dati personali le persone giuridiche, gli enti e le associazioni). Pertanto l'amministrazione è stata invitata a motivare in maniera congrua e completa in ordine alla sussistenza del pregiudizio concreto alla protezione dei dati personali anche perché la stessa si era limitata a richiamare il citato provvedimento 14 giugno 2018, n. 382, senza specificare perché la tipologia degli atti richiesta sarebbe stata "idonea a rivelare dati di carattere sensibile" o "il tenore di vita e la situazione economica personale" degli interessati. A tal fine è stata in ogni caso ricordata la necessità di tenere conto del regime amplificato di pubblicità dell'accesso civico generalizzato, del principio di "minimizzazione" dei dati personali (art. 5, par. 1, lett. *c*), del RGPD), delle ragionevoli aspettative di confidenzialità dei controinteressati in relazione al momento in cui i dati sono stati raccolti, nonché della prevedibilità, al momento della raccolta, delle conseguenze derivanti dall'eventuale conoscibilità da parte di chiunque degli stessi dati, anche valutando che la richiesta era riferibile a documentazione molto risalente, e l'istante non aveva circoscritto la propria richiesta a un preciso arco temporale, ma a "tutte" le tasse e i canoni percepiti dal comune per l'occupazione di spazi e aree pubbliche (parere 24 dicembre 2018, n. 519, doc. web n. 9073654).

Accesso ai verbali della Polizia municipale

Il Garante è intervenuto rispetto al diniego opposto a un'istanza di accesso civico a verbali di accertamento della Polizia municipale emessi per fatti avvenuti, in alcune date specificamente indicate, nei confronti di esercizi di pubblico ristoro che si sono opposti all'ostensione, affermando che sono sottratte dall'ambito di applicazione della disciplina in materia di protezione dei dati personali le persone giuridiche, gli enti e le associazioni, che non possono beneficiare della tutela di cui al citato art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (parere 12 aprile 2018, n. 214, doc. web n. 8790479). È stato inoltre aggiunto che, laddove, invece, i dati presenti all'interno della documentazione di cui si chiedeva l'accesso fossero da intendersi come riferiti ad altri soggetti (persone fisiche), l'amministrazione destinataria dell'istanza di accesso civico era tenuta a verificare se l'accesso civico doveva essere rifiutato per evitare un pregiudizio concreto alla tutela della protezione dei dati personali, seguendo, a tale scopo, le indicazioni fornite nelle citate Linee guida dell'Anac in materia di accesso civico.

Per altro verso, in relazione a un'altra istanza di accesso civico ai verbali di accertamento emessi dalla Polizia municipale in una data zona e in un determinato lasso di tempo, è stato affermato che l'amministrazione aveva correttamente concesso l'accesso parziale al solo dato numerico aggregato. Diversamente, infatti, l'ostensione della copia dei documenti richiesti, contenendo molteplici informazioni personali, quali, in linea generale, nominativo, residenza, targa dell'autoveicolo, data e luogo della violazione, importo della sanzione, ecc., avrebbe comportato un pregiudizio concreto alla protezione dei dati personali alla luce del quale l'accesso civico va

4

rifiutato ai sensi dell'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (parere 18 gennaio 2018, n. 15, doc. web n. 7689066).

Diversamente, in un altro parere, di fronte al diniego opposto ad un'istanza di accesso civico, formulata dal sindaco di un comune alla provincia di riferimento e volta a conoscere i nomi degli altri comuni eventualmente protagonisti di analoghi accertamenti di natura sanzionatoria, sinteticamente motivata e senza il coinvolgimento dei controinteressati, il Garante ha ritenuto opportuno che la provincia rivalutasse la richiesta di accesso civico ai dati richiesti, previo coinvolgimento dei controinteressati, fornendo, altresì, nella risposta, una motivazione congrua e completa rispetto all'esistenza o meno del limite della protezione dei dati personali di cui al decreto legislativo n. 33/2013 (parere 12 aprile 2018, n. 216, doc. web n. 8811865).

Permessi per veicoli

In un caso di accesso civico ad atti relativi agli *iter* concessori della polizia municipale per la realizzazione di spazi di sosta personalizzati destinati a soggetti disabili, nonché alle dichiarazioni rese da questi ultimi, il Garante ha ritenuto corretto il rifiuto opposto all'istanza (parere 16 aprile 2018, n. 226, doc. web n. 8983848). Ciò in quanto i documenti richiesti contenevano dati sensibili, idonei a rivelare lo stato di salute degli interessati (i soggetti disabili aventi diritto all'area di sosta personalizzata). È stato pertanto evidenziato che tale fattispecie rientrava in una delle ipotesi di "esclusione" dell'accesso civico previste dal decreto legislativo n. 33/2013, stante il "divieto di divulgazione" dei dati sulla salute, previsto dalla normativa in materia di protezione dei dati personali (cfr. oggi art. 2-*septie*s, comma 8, del Codice che ricalca il previgente art. 22, comma 8; cfr. anche art. 7-*bis*, comma 6, d.lgs. n. 33/2013).

In un'altra situazione, a fronte di un'istanza di accesso civico generalizzato avente a oggetto la documentazione relativa all'accesso e alla sosta in zone a traffico limitato (Ztl), è stata condivisa la decisione dell'amministrazione che aveva concesso il solo accesso parziale agli atti non contenenti dati personali. Rispetto invece alla documentazione inerente ai soggetti autorizzati al transito e alla sosta nelle Ztl, è stato rappresentato che il comune aveva correttamente negato l'accesso, posto che la stessa contiene informazioni qualificabili come dati personali (es., oltre ai nominativi, anche gli indirizzi di residenza, i numeri di telefono, nonché gli indirizzi di posta elettronica), la cui diffusione può determinare una interferenza ingiustificata nei diritti e libertà dei controinteressati, con possibili ripercussioni negative sul piano professionale, personale e sociale. Pertanto, tenendo anche conto delle ragionevoli aspettative di confidenzialità dei soggetti in relazione al trattamento dei propri dati personali al momento in cui essi sono stati raccolti dal comune, delle conseguenze derivanti dalla conoscibilità da parte di chiunque dei dati richiesti, nonché del ristretto ambito territoriale, l'ostensione dei citati documenti poteva arrecare ai controinteressati un pregiudizio concreto alla tutela della protezione dei dati personali ai sensi dall'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (parere 31 agosto 2018, n. 450, doc. web n. 9045220).

Dati sulla salute

Quanto all'accesso civico a dati sulla salute, il Garante ha confermato i precedenti orientamenti evidenziando che deve essere "escluso" l'accesso civico a dati sulla salute (nel caso di specie informazioni legate all'attività lavorativa, quali cause di assenza dal servizio e dettagli sullo stato di salute, nonché su prescrizioni mediche dei soggetti citati nella documentazione oggetto di accesso) ai sensi dell'art. 5-*bis*, comma 3, d.lgs. n. 33/2013. Ciò in ragione di un espresso divieto di diffusione di tali informazioni (cfr. art. 22, comma 8, d.lgs. n. 196/2003, oggi abrogato ma i cui contenuti sono stati riportati nel nuovo art. 2-*septies*, comma 8, del Codice) (parere 22 febbraio 2018, n. 98, doc. web n. 8165944).

Operazioni Sar

Il Garante è stato chiamato a fornire parere anche su un caso di accesso civico a operazioni *Search and Rescue* (Sar). In particolare, è stato ritenuto corretto il diniego

di accesso civico ai numeri di telefono e ai nominativi dei soggetti coinvolti (es., segnalanti e destinatari della segnalazione, italiani ed esteri, coinvolti nelle operazioni di ricerca e salvataggio) contenuti nella documentazione detenuta dal Comando generale del Corpo delle capitanerie di porto, inerente un'operazione Sar relativa alla richiesta di soccorso di un natante in difficoltà, navigante nel Mar Libico con a bordo migranti (parere 3 maggio 2018, n. 259, doc. web n. 8997292). Ciò in quanto la loro ostensione era suscettibile di arrecare ai controinteressati il pregiudizio concreto alla tutela della protezione dei dati personali previsto dalla norma in materia di accesso civico.

Autorizzazioni comunali anche paesaggistiche

È stato reso parere anche su un'istanza di accesso civico avente a oggetto dati e informazioni personali di coloro che hanno chiesto autorizzazioni per l'impianto di nuovi vigneti, corredati anche dei relativi dati catastali, ritenendo corretto il rigetto opposto dall'amministrazione. Ciò considerando che l'ostensione dei dati e delle informazioni richieste poteva determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei controinteressati, con possibili ripercussioni negative sul piano personale e sociale. In tale occasione, non è stato ritenuto possibile fornire nemmeno un accesso civico parziale, limitato alla documentazione priva dei nominativi dei controinteressati, in quanto le informazioni contenute nella documentazione richiesta, quali fra l'altro i dati catastali, consentivano comunque di risalire ai dati identificativi del relativo proprietario, attraverso il collegamento con le informazioni contenute in altre banche dati (es., banca dati catastale gestita dall'Agenzia delle entrate) (parere 19 luglio 2018, n. 426, doc. web n. 9027184).

In un'altra occasione, invece, è stato reso un parere in materia accesso civico ad autorizzazioni paesaggistiche rilasciate a una società, evidenziando che sono sottratte dall'ambito di applicazione della disciplina in materia di protezione dei dati personali le persone giuridiche, gli enti e le associazioni, che non possono beneficiare della tutela di cui al citato art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (cfr. anche considerando n. 14 del RGPD). Pertanto nel caso esaminato è stato rappresentato che laddove i dati contenuti nei documenti di cui si chiedeva l'ostensione fossero stati riferiti a persone giuridiche, la disciplina sulla protezione dei dati non poteva applicarsi, essendo la nozione di "dato personale" riferita esclusivamente alle persone fisiche. Inoltre, nel caso di specie il comune aveva negato l'ostensione dei documenti sulla base dell'esistenza di un pregiudizio concreto alla protezione dei dati personali, considerando la quantità e la qualità di dati personali coinvolti, senza tuttavia specificare quali fossero effettivamente i dati in questione (di cui non veniva fornita una descrizione neanche di tipo generale), con la conseguenza che la motivazione contenuta nel provvedimento di diniego non consentiva di comprendere le effettive ragioni per cui il rilascio avrebbe determinato un pregiudizio concreto ai sensi all'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (parere 7 settembre 2018, n. 451, doc. web n. 9045244).

Alienazione di immobile comunale

Il Garante si è espresso a fronte di un'istanza di accesso civico volta a ottenere copia dell'intero fascicolo relativo all'alienazione di un immobile comunale con vincolo di destinazione decennale a favore di una persona fisica. Nella fattispecie considerata il Comune destinatario dell'istanza è stato invitato a valutare la possibilità di accordare un accesso civico parziale ai soli documenti inerenti all'atto di compravendita e alla deliberazione autorizzativa dell'alienazione, previo oscuramento dei dati personali (e di tutte le altre informazioni capaci di identificare, anche indirettamente, il controinteressato) ivi menzionati (compresi quelli dei soggetti non intervenuti nel procedimento di accesso civico) e dei dati identificativi e catastali dell'immobile venduto riportati nei predetti documenti. Tutto ciò avuto riguardo anche al limitato regime di pubblicità della deliberazione autorizzativa dell'alienazione – allegata all'atto di compravendita, che peraltro ne riproduceva anche i contenuti essen-

4

ziali – la quale, secondo quanto riferito, era stata già oggetto di pubblicazione all'albo pretorio nel 2005, per i quindici giorni previsti dalla normativa di settore (art. 124, comma 1, d.lgs. 18 luglio 2000 n. 267). È stata inoltre ritenuta corretta l'esclusione della relazione di servizio dell'architetto comunale e delle missive poiché l'ostensione di tali documenti poteva arrecare un pregiudizio concreto ai diritti e alle libertà del controinteressato, considerato il livello di conflittualità insorto tra lo stesso e il comune (parere 26 luglio 2018, n. 448, doc. web n. 9027200).

Onere di motivazione

Il Garante è stato chiamato a rendere parere anche in relazione a un'istanza di accesso civico alla relazione di indagine della commissione interna delle Ferrovie Sud Est relativa a un incidente ferroviario avvenuto nel 2017, nonché agli esiti delle interviste che la Commissione aveva effettuato con il personale ferroviario coinvolto. In tale circostanza, è stato ritenuto che, in entrambi i casi, il rifiuto era fondato su motivazioni diverse da quelle per le quali è previsto l'obbligo di chiedere il parere formale al Garante. È stato poi evidenziato che, nonostante il responsabile della trasparenza avesse richiamato generici motivi di *privacy* che avrebbero potuto portare al rifiuto dell'ostensione della documentazione richiesta, non risultavano specificati – né nella predetta nota, né in altri atti dell'istruttoria – quali sarebbero stati i dati personali coinvolti. Pertanto, richiamando le già citate Linee guida dell'Anac in materia di accesso civico, è stato ricordato che nella risposta negativa o parzialmente tale, sia per i casi di diniego connessi all'esistenza di limiti di cui ai commi 1 e 2 che per quelli connessi all'esistenza di casi di esclusione di cui all'art. 5-*bis*, comma 3, l'amministrazione era tenuta a una congrua e completa, motivazione. Quest'ultima serve all'amministrazione per definire progressivamente proprie linee di condotta ragionevoli e legittime e al cittadino per comprendere ampiezza e limiti dell'accesso generalizzato, nonché le decisioni dell'amministrazione (parere 11 ottobre 2018, n. 465, doc. web n. 9063945).

Procedimenti disciplinari

Il Garante ha esaminato una richiesta di riesame di un provvedimento di rifiuto di accesso civico alla deliberazione di un istituto di ricovero e cura (Irccs) relativa al procedimento disciplinare nei confronti di un proprio dipendente. Sul punto è stato osservato che all'interno del testo della deliberazione oggetto dell'accesso civico erano presenti una serie di dati delicati e di informazioni personali afferenti al rapporto di lavoro dell'interessato e, per tale ragione, è stato ritenuto corretto il rifiuto opposto dall'Istituto alla predetta documentazione, in quanto la relativa ostensione avrebbe potuto arrecare all'interessato un concreto pregiudizio alla tutela dei propri dati, con evidenti ripercussioni sul piano sociale e personale (parere 21 novembre 2018, n. 483, doc. web n. 9065404).

Iscrizione temporanea presso un'azienda sanitaria

Altro parere è stato emesso in un caso di richiesta di riesame di un provvedimento di rifiuto di un accesso civico attraverso il quale si desiderava conoscere se un soggetto identificato fosse titolare di un'iscrizione temporanea presso un'azienda sanitaria. Il Garante ha ritenuto che l'istanza di accesso civico fosse stata correttamente respinta, in quanto l'ostensione delle informazioni richieste era suscettibile di arrecare un serio e concreto pregiudizio alla tutela dei dati personali dell'interessato. Infatti, la generale conoscenza delle informazioni personali relative all'effettuazione dell'iscrizione temporanea presso la Ausl con la data di decorrenza – permessa solo a coloro che permangono nel comune di domicilio per un periodo "superiore ai tre mesi" per "motivi di lavoro, di studio, di salute, familiari, per disoccupazione, per soggiorno obbligato o libertà provvisoria" – poteva determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dell'interessato, con possibili ripercussioni negative sul piano personale, relazionale e sociale (parere 13 dicembre 2018, n. 501, doc. web n. 9073707).

Diploma di laurea

Il Garante si è espresso anche in relazione a una richiesta di accesso civico generalizzato avente a oggetto "l'attestazione del conseguimento della laurea in

Giurisprudenza con indicazione della data della seduta pubblica o in alternativa della copia del diploma di laurea”. Al riguardo è stato evidenziato che il rilascio di certificati da parte delle Università resta disciplinato dalla specifica normativa di settore per il quale agli uffici pubblici è vietato rilasciare, persino all’interessato, certificati da esibire ad altre pubbliche amministrazioni e ai gestori di pubblici servizi (art. 40, d.P.R. 28 dicembre 2000, n. 445). Ciò anche perché le certificazioni rilasciate dalla pubblica amministrazione in ordine a stati, qualità personali e fatti sono valide ed utilizzabili solo nei rapporti tra privati e per il rilascio di ciascun certificato è previsto, in ogni caso, il pagamento dell’imposta di bollo e dei diritti di segreteria ai sensi del d.P.R. 26 ottobre 1972, n. 642, a esclusione degli usi ivi indicati. Nei rapporti con gli organi della pubblica amministrazione e i gestori di pubblici servizi, i certificati e gli atti di notorietà sono sempre sostituiti dalle dichiarazioni sostitutive. Le amministrazioni pubbliche e i gestori di pubblici servizi “sono tenuti ad acquisire d’ufficio le informazioni oggetto delle dichiarazioni sostitutive di cui agli artt. 46 e 47, nonché tutti i dati e i documenti che siano in possesso delle pubbliche amministrazioni, previa indicazione, da parte dell’interessato, degli elementi indispensabili per il reperimento delle informazioni o dei dati richiesti, ovvero ad accettare la dichiarazione sostitutiva prodotta dall’interessato” (art. 43, comma 1, d.P.R. n. 445/2000).

Pertanto, in tale quadro, è stato rappresentato all’Università istante che il rilascio del certificato di laurea è sottoposto a regole specifiche, che non possono essere superate tramite la disciplina sull’accesso civico, sia nel caso che a richiedere il certificato sia l’interessato, come pure, a maggior ragione, un terzo. La citata disciplina di settore contenuta nel d.P.R. n. 445/2000 non è quindi derogabile dalle disposizioni contenute nel decreto legislativo n. 33/2013, che peraltro prevedono espressamente che l’accesso civico debba essere “escluso” nei casi in cui “è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti”. Inoltre, nel caso di specie risultava che il *curriculum* del controinteressato era stato pubblicato sul sito web dell’amministrazione di appartenenza, con indicazione del titolo di studio universitario conseguito, e che pertanto, in tale contesto e ai sensi della normativa richiamata, era la p.a. – e non un terzo privato – tenuta ad acquisire d’ufficio le informazioni oggetto delle dichiarazioni sostitutive presentate, per verificare la veridicità dei titoli dichiarati (art. 43, comma 1, d.P.R. n. 445/2000) (parere 9 maggio 2018, n. 278, doc. web n. 9099910).

4.2.2. La pubblicazione di dati personali online

In materia di diffusione di dati personali *online* per finalità di trasparenza o di pubblicità dell’azione amministrativa, nel dare riscontro a reclami, segnalazioni e quesiti il Garante è stato chiamato a pronunciarsi su numerose questioni, di cui si riportano solo i casi più rilevanti conclusi con provvedimento del Collegio. In particolare, si richiama ancora una volta il problema della diffusione *online* da parte di soggetti pubblici in assenza di un idoneo presupposto normativo (norma di legge o di regolamento).

Il Garante ha in proposito censurato il comportamento di un comune che aveva pubblicato sul sito web istituzionale, nella sezione denominata “Accesso agli atti amministrativi”, una determinazione con la quale era stato stabilito l’obbligo del segnalante (dipendente comunale) di astenersi, su propria richiesta, dalla valutazione di altra dipendente a cui risultava legato da rapporto di coniugio, per potenziale conflitto di interessi. La determinazione, che risultava *online* da quasi tre anni, riportava in chiaro dati e informazioni personali del segnalante e della moglie, quali, oltre i dati identificativi dei coniugi, informazioni sull’esistenza di un rap-

porto di lavoro presso l'ente e di un potenziale conflitto di interessi. È stata pertanto rilevata l'illiceità del trattamento di dati personali effettuato dal comune, in quanto avvenuto in maniera non conforme alla disciplina rilevante in materia di protezione dei dati personali, essendo stati diffusi dati personali sul web in assenza di un idoneo presupposto normativo per il periodo superiore ai 15 giorni di pubblicazione previsti dalla normativa di settore (art. 19, comma 3, d.lgs. n. 196/2003, oggi abrogato ma i cui contenuti sono stati riprodotti nel nuovo art. 2-*ter*, commi 1 e 3, del Codice) secondo la quale "Tutte le deliberazioni del comune e della provincia sono pubblicate mediante pubblicazione all'albo pretorio, nella sede dell'ente, per quindici giorni consecutivi, salvo specifiche disposizioni di legge" (art. 124, comma 1, d.lgs. 18 agosto 2000, n. 267) (provv. 16 maggio 2018, n. 292, doc. web n. 8998347).

4.3. *La documentazione anagrafica e la materia elettorale*

4.3.1. Indicazione "padre" e "madre" sulla Cie

Il Ministero dell'interno ha richiesto il parere del Garante su un decreto con il quale si intendeva apportare modifiche al d.m. 23 dicembre 2015, recante "Modalità tecniche di emissione della Carta d'identità elettronica", consistenti nell'inserimento, nella disposizione relativa alle modalità di presentazione della richiesta della carta di identità elettronica per il minore da parte dei genitori e nell'allegato che disciplina le informazioni da riportare sul documento, delle parole "padre" e "madre", in luogo di "genitori".

Il Ministero, a fronte delle modifiche proposte, ha rappresentato la necessità di un adeguamento alla normativa sullo stato civile, in particolare al decreto del 23 dicembre 2015 per quanto attiene alla "qualificazione dei soggetti legittimati a presentare agli ufficiali d'anagrafe la richiesta di emissione del documento elettronico in favore di minori di età", in un contesto di complessiva coerenza nell'esercizio delle funzioni statali delegate.

L'Autorità, considerato che la situazione giuridica soggettiva che rileva nella fattispecie interessata dall'intervento normativo è la titolarità della responsabilità genitoriale o della potestà tutoria, ha evidenziato che la modifica proposta avrebbe introdotto, *ex novo*, profili di criticità nei casi in cui la richiesta della carta di identità, per un minore, fosse presentata da figure esercenti la responsabilità genitoriale che non fossero esattamente riconducibili alla specificazione terminologica "padre" o "madre". Ciò, in particolare, nei casi in cui la responsabilità genitoriale e la successiva trascrizione nei registri dello stato civile consegua a una pronuncia giurisdizionale (sentenza di adozione in casi particolari, ex art. 44, l. n. 184/1983, trascrizione di atti di nascita formati all'estero, riconoscimento in Italia di provvedimento di adozione pronunciato all'estero, rettificazione di attribuzione di sesso, *ex lege* n. 164/1982) oppure sia effettuata direttamente dal Sindaco, senza necessità di ricorso all'autorità giudiziaria. In tali ipotesi, la modifica ipotizzata non contemplerebbe la possibilità di una richiesta congiunta della carta di identità per il minore (valida per l'espatrio) da parte di figure genitoriali non esattamente riconducibili alla specificazione terminologica "padre" o "madre" e, di conseguenza, l'esercizio del diritto potrebbe essere impedito dall'ufficio – in violazione di legge – oppure essere subordinato a una dichiarazione, non corrispondente alla realtà, da parte di uno degli esercenti la responsabilità genitoriale. All'atto della richiesta del documento di identità del minore, la sostituzione terminologica proposta potrebbe imporre ai dichiaranti il conferimento di dati inesatti o di delicate informazioni non necessarie di

carattere personale, arrivando in alcuni casi a escludere il rilascio del documento a fronte di dichiarazioni non corrispondenti alla situazione di fatto derivante dalla particolare composizione del nucleo familiare.

Infine, come anche osservato dal Ministero nella relazione illustrativa, il documento di identità deve riportare i dati anagrafici come risultanti dalla relativa scheda anagrafica tenuta dal comune di residenza, conformi ai rispettivi elementi degli atti dello stato civile e, in particolare, alla disciplina degli atti di nascita riferita alla madre ed al padre nonché dei relativi registri. Nella procedura prevista per il rilascio della carta di identità, la verifica della correttezza dei dati e della sussistenza della responsabilità genitoriale (o della potestà tutoria) è oggetto di uno specifico accertamento da parte del funzionario comunale preposto, per quanto attiene alla loro corrispondenza con quanto risulta nei registri anagrafici e di stato civile.

Per tali ragioni, l'Autorità nel rilasciare il parere nei termini sopra indicati, ha richiamato l'attenzione del Ministero sulla necessità che le norme che disciplinano il rilascio della carta di identità elettronica debbano essere idonee ad assicurare l'esattezza dei dati verificati dall'ufficiale di stato civile nei relativi registri (provv. 31 ottobre 2018, n. 476, doc. web n. 9058965).

4.3.2. Referendum *e invio di materiale propagandistico*

Nel corso dell'anno sono state concluse numerose istruttorie, avviate nel 2017 a seguito delle segnalazioni pervenute in occasione della campagna per il *referendum* costituzionale del 4 dicembre 2016, riguardanti l'invio di materiale informativo, sia per posta che a mezzo e-mail, a cittadini residenti in Italia e all'estero, da parte dei diversi soggetti (comitati referendari e partiti).

Una delle segnalazioni pervenute ha riguardato la ricezione di un opuscolo di propaganda per il *referendum*, riportante la firma del presidente di una regione. Il predetto materiale informativo riportava, quale riferimento al quale rivolgersi per l'esercizio dei propri diritti, l'indirizzo web relativo a un sito istituzionale facente capo alla regione.

L'istruttoria ha consentito di accertare che, sebbene il sito web indicato fosse senz'altro riferibile alla regione – si trattava di un sito informativo dedicato alla divulgazione dell'azione amministrativa e all'attuazione del programma politico del presidente e della giunta regionale –, i trattamenti di dati personali relativi alla campagna di comunicazione per il *referendum* non erano stati effettuati con l'impiego di risorse umane o strumentali facenti capo all'ente pubblico. La campagna comunicativa in questione era stata, infatti, gestita direttamente dalla sede territoriale del partito, cui faceva riferimento il comitato referendario, che aveva curato sia la predisposizione del materiale informativo, sia l'acquisizione e il successivo trattamento dei dati personali necessari per l'invio degli opuscoli agli elettori. All'esito degli accertamenti, che hanno individuato la titolarità del trattamento in capo alla sede territoriale del partito, sono emerse violazioni del provvedimento in materia di trattamento di dati personali presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale, adottato dal Garante il 6 marzo 2014, n. 107 (doc. web n. 3013267). In particolare, non è stata rispettata, ai fini dell'esonero dall'informativa, la condizione che richiede che nel materiale inviato sia chiaramente indicato un recapito (indirizzo postale, e-mail, eventualmente anche con rinvio a un sito web dove tali riferimenti siano facilmente individuabili) al quale l'interessato possa agevolmente rivolgersi per esercitare i diritti di cui all'art. 7 del Codice" (punto 5.1, provv. cit.). L'opuscolo oggetto della segnalazione, infatti, non riportava alcun recapito del titolare, e l'Ufficio non ha ritenuto a tal fine idoneo il riferimento al sito web della regione e il logo relativo al comitato nazionale promotore della campagna

(nota 18 aprile 2018). Quale effetto della riscontrata violazione è stato avviato un procedimento sanzionatorio, definito con provvedimento 25 ottobre 2018, n. 474 (doc. web n. 9090257).

Un'altra istruttoria ha riguardato il caso di un medico oncologo che aveva inviato a suoi ex pazienti, visitati o seguiti nel corso della sua attività professionale presso un istituto di cura, una missiva con la quale comunicava il suo sostegno a un candidato – già assessore regionale alla sanità – in occasione di una consultazione regionale. Tale trattamento è stato ritenuto illecito in quanto effettuato dal medico in assenza di informativa e consenso per le specifiche finalità di propaganda elettorale. I dati dei pazienti, circa 3.500 contatti, erano stati acquisiti dal medico all'atto della cessazione del rapporto con la struttura sanitaria presso la quale prestava la sua attività in regime di libera professione. L'informativa resa a suo tempo e il consenso acquisito per finalità di cura dalla struttura sanitaria, non sono stati ritenuti validi presupposti per il successivo utilizzo dei dati da parte di un soggetto diverso (il libero professionista) e per finalità completamente differenti, come quelle di promozione politico-elettorale di cui alla missiva in esame. Ritenuta pertanto sussistente la violazione degli artt. 13, comma 4, 23 e 26, d.lgs. n. 196/2003, l'Ufficio ha avviato un autonomo procedimento sanzionatorio (nota 1° agosto 2018).

4.4. *L'istruzione scolastica*

Nel settore scolastico il Garante ha interagito sia con il Miur che con università, istituzioni scolastiche ed altri soggetti pubblici nel corso di incontri e contatti volti a fornire chiarimenti e indicazioni in merito alla corretta applicazione della nuova disciplina in materia di protezione dei dati personali (on riguardo anche a Invalsi e Crui).

In tale ambito, particolare rilievo ha assunto il provvedimento del 15 febbraio 2018, n. 76 (doc. web n. 8081291) con il quale il Garante ha espresso, ai sensi degli artt. 20, comma 2, e 154, comma 1, lett. *g*), d.lgs. n, 196/2003, parere favorevole sullo schema di regolamento relativo alle modalità di svolgimento delle prove Invalsi del terzo anno della scuola secondaria di primo grado, in attuazione del decreto legislativo 13 aprile 2017, n. 62. Quest'ultimo stabilisce che Invalsi effettua rilevazioni nazionali attraverso prove standardizzate, *computer based*, volte ad accertare i livelli generali e specifici di apprendimento conseguiti in italiano, matematica e inglese e che la partecipazione a tali rilevazioni rappresenta requisito di ammissione all'esame conclusivo del primo ciclo di istruzione. Lo schema di regolamento stabilisce procedure e regole relative allo svolgimento delle prove Invalsi della "terza media" e disciplina, in particolare: le modalità di identificazione dello studente ai fini del corretto espletamento e della restituzione delle prove che, nel caso di alunni con disabilità (Dva) e di alunni con disturbi specifici di apprendimento (Dsa), possono essere personalizzate; lo svolgimento delle prove, prevedendo che Invalsi predisponga un documento contenente informazioni che consentono la sicura identificazione di ciascuno studente; le modalità e i tempi di conservazione dei dati da parte di Invalsi, prevedendo la cancellazione del nome e del cognome degli studenti una volta terminato lo svolgimento delle prove.

Lo schema di decreto presentato ha tenuto conto degli approfondimenti effettuati nel corso di incontri di lavoro tenutisi con i rappresentanti di Invalsi e del Miur, volti a rendere lo schema in esame conforme alla disciplina vigente grazie all'adozione di misure tecniche e organizzative volte ad assicurare la protezione dei dati personali per impostazione predefinita. In particolare, facendo seguito alle osservazioni

rese dall'Autorità, Invalsi ha riformulato lo schema di regolamento con particolare riferimento a: l'individuazione, nel rispetto dei principi di pertinenza e non eccedenza, delle informazioni personali da utilizzare per l'identificazione degli studenti, la valutazione, la somministrazione e la restituzione delle prove; la limitazione dei tempi di conservazione dei dati, sia con riferimento al nome e al cognome, che in relazione ai dati idonei a rivelare lo stato di salute relativi allo svolgimento delle prove personalizzate da parte degli studenti con Dva e con Dsa; la necessità di adottare, in relazione ai dati idonei a rivelare lo stato di salute, tecniche crittografiche al fine di rendere tali dati inintelligibili, nonché di conservarli in partizioni separate; l'adozione di idonee misure di sicurezza, in particolare, nello scambio di dati personali tra Miur ed Invalsi, nel rispetto delle misure necessarie già prescritte dal Garante con il provvedimento generale 2 luglio 2015, n. 393 (doc. web n. 4129029).

L'Ufficio ha ricevuto inoltre numerosi reclami e segnalazioni aventi ad oggetto la diffusione, sul sito web istituzionale di taluni istituti scolastici, di graduatorie d'istituto relative al personale docente o al personale Ata, contenenti anche informazioni relative all'indirizzo di residenza, al numero di telefono fisso o di cellulare e all'indirizzo e-mail del personale. Tali informazioni, in alcuni casi, sarebbero state indicizzate anche sui comuni motori di ricerca. A seguito degli approfondimenti effettuati, è stato riscontrato che tali graduatorie contenevano anche l'indicazione dei titoli di preferenza del personale scolastico e, tra questi, in particolare, dati relativi alla salute dei docenti, contrariamente a quanto previsto dalla disciplina di protezione dei dati che vieta esplicitamente la diffusione di tali informazioni. Grazie all'intervento dell'Autorità, gli istituti scolastici hanno prontamente rimosso tali dati dal sito istituzionale.

L'Ufficio ha inoltre ricevuto una segnalazione con la quale si rappresentava che nei moduli di iscrizione a scuola, anche dell'infanzia, in Alto Adige veniva richiesto di fornire anche informazioni relative alla madrelingua di appartenenza. È stata quindi avviata un'istruttoria preliminare volta a verificare la compatibilità del trattamento segnalato con la disciplina di protezione dei dati e con lo specifico quadro di garanzie previsto per il trattamento di quelli relativi all'appartenenza/aggregazione ai tre gruppi linguistici italiano, tedesco e ladino in provincia di Bolzano.

La Provincia autonoma di Bolzano, a seguito degli approfondimenti effettuati dall'Ufficio, ha chiarito che non vengono raccolti dati relativi alla madrelingua o altre informazioni che rivelino l'origine razziale o etnica dei minori o delle famiglie di appartenenza, ma che, all'atto dell'iscrizione nelle scuole, vengono richiesti i dati sulle lingue conosciute dagli alunni (italiano, tedesco o altra), senza specificare alcuna preferenza, ma indicando solo il livello di conoscenza di ciascuna lingua (ottimo, buono, sufficiente o insufficiente). Tale trattamento è necessario al fine di permettere all'istituto scolastico presso il quale l'alunno sarà iscritto di organizzare più efficacemente l'attività didattica, anche in sede di formazione delle classi.

Nell'ambito delle interlocuzioni con l'Ufficio, la Provincia ha inoltre individuato soluzioni tecniche e organizzative a tutela dei diritti e delle libertà degli interessati volte a rendere il trattamento in esame conforme alla disciplina in materia di protezione dei dati personali (nota 20 dicembre 2018).

4.5. *L'attività fiscale e tributaria*

4.5.1. La dichiarazione dei redditi "precompilata"

Anche nel 2018 il Garante è intervenuto con numerosi pareri nell'ambito del percorso di attuazione normativa della cd. dichiarazione precompilata da parte del

4

Mef e dell'Agenzia delle entrate. In relazione all'ampliamento delle informazioni da comunicare all'Agenzia delle entrate per la precompilazione della dichiarazione dei redditi, il Garante si è espresso favorevolmente su due schemi di decreto del Mef, attuativi dell'art. 3, comma 4, d.lgs. n. 175/2014, concernenti la trasmissione all'Agenzia delle entrate dei dati riguardanti le spese relative alle rette per la frequenza di asili nido e dei dati relativi alle erogazioni liberali in favore delle Onlus, delle associazioni di promozione sociale e delle fondazioni e associazioni aventi per scopo statutario la tutela, promozione e la valorizzazione dei beni di interesse artistico, storico e paesaggistico, nonché lo svolgimento o la promozione di attività di ricerca scientifica (v. pareri 11 gennaio 2018, nn. 1 e 2, rispettivamente doc. web nn. 7936278 e 7925253).

In particolare, in relazione ai dati relativi alle erogazioni liberali, il Garante ha rilevato che tale trattamento ha per oggetto anche informazioni di carattere sensibile, idonee a rivelare, in particolare, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, nonché lo stato di salute e la vita sessuale. Pertanto, nel menzionato parere, a fronte del previsto invio facoltativo all'Agenzia delle entrate, da parte delle predette organizzazioni, delle informazioni concernenti le erogazioni liberali ricevute, tenuto conto del carattere sperimentale della misura – per gli anni di imposta 2017, 2018 e 2019 –, l'Autorità ha evidenziato la necessità che, nel provvedimento attuativo del Direttore dell'Agenzia delle entrate, concernente la definizione delle modalità tecniche di trasmissione delle informazioni, siano individuate particolari garanzie a tutela dei diritti e delle libertà fondamentali garantendo anche agli interessati la volontarietà dell'adesione alla trasmissione di tali informazioni sensibili all'Agenzia delle entrate.

In seguito il Garante ha espresso parere favorevole sui conseguenti schemi di provvedimenti attuativi del Direttore dell'Agenzia delle entrate relativi alla raccolta delle spese sostenute per asili nido ed erogazioni liberali, che tengono conto degli approfondimenti effettuati con i rappresentanti dell'Agenzia delle entrate, al fine di assicurare il rispetto della disciplina di protezione dei dati, con particolare riferimento alla pertinenza e non eccedenza dei dati raccolti (provv. 8 febbraio 2018, n. 66, doc. web n. 7772714).

Inoltre, particolare attenzione è stata posta alla tutela dei diritti dei contribuenti, prevedendo per chiunque ne abbia interesse la possibilità di esercitare presso l'Agenzia delle entrate la propria opposizione all'inserimento di tali spese nella dichiarazione precompilata. In merito alle erogazioni liberali sono state introdotte maggiori cautele per gli interessati, in considerazione della delicatezza delle informazioni oggetto di comunicazione, individuando specifiche modalità di conservazione dei dati, ristretti tempi di conservazione e un termine più esteso per l'esercizio dell'opposizione, necessario soprattutto con riferimento alle informazioni relative all'anno di imposta 2017, nonché la possibilità di esercitare l'opposizione, a partire dall'anno di imposta 2018, che può essere fatta valere anche direttamente nei confronti del soggetto che riceve l'erogazione. È stato altresì richiesto all'Agenzia di individuare correttamente, limitando le finalità del trattamento di tali informazioni (anche sensibili) all'elaborazione della dichiarazione precompilata, escludendo che, in caso di esercizio del diritto di opposizione, i dati comunicati dalle organizzazioni possano essere trattati anche per finalità di controllo sugli oneri deducibili e detraibili ai sensi dell'art. 7, comma 5, d.P.R. n. 605/1973. È stato inoltre ritenuto necessario l'avvio di un'idonea campagna informativa attraverso il sito web dell'Agenzia delle entrate e altri strumenti di informazione per rendere note ai contribuenti le modalità di esercizio dell'opposizione.

Infine, atteso il carattere sperimentale della raccolta dei dati relativi alle eroga-

zioni liberali, il cui conferimento è facoltativo, il Garante ha chiesto all'Agenzia di valutare l'efficacia delle misure introdotte a garanzia dei diritti e delle libertà fondamentali, nonché della dignità degli interessati. Una volta conclusa la fase di sperimentazione, tale valutazione dovrà essere sottoposta all'esame dell'Autorità prima di disciplinare a regime la raccolta delle predette informazioni.

Il Garante ha espresso parere favorevole anche su quattro schemi di provvedimento del Direttore dell'Agenzia delle entrate, integrativi di rispettivi precedenti provvedimenti, che disciplinano la comunicazione all'anagrafe tributaria di informazioni per l'elaborazione della dichiarazione precompilata con riferimento ai dati relativi agli interventi di recupero del patrimonio edilizio e di riqualificazione energetica effettuati su parti comuni di edifici residenziali, ai pagamenti effettuati a mezzo bonifico per interventi di recupero del patrimonio edilizio e di riqualificazione energetica degli edifici, alle spese sanitarie rimborsate, nonché ai contributi versati alle forme pensionistiche complementari di cui al decreto legislativo 5 dicembre 2005, n. 252. Le modifiche apportate dall'Agenzia hanno riguardato esclusivamente le tipologie di informazioni oggetto di comunicazione, senza alcuna modifica dei canali di trasmissione e delle relative misure di sicurezza (parere 1° febbraio 2018, n. 44, doc. web n. 7772512).

Spese sanitarie nella dichiarazione precompilata

Con specifico riferimento alle spese sanitarie, il Garante è intervenuto sullo schema di provvedimento del Direttore dell'Agenzia delle entrate recante "Modalità tecniche di utilizzo dei dati delle spese sanitarie ai fini della elaborazione della dichiarazione dei redditi precompilata, a decorrere dall'anno d'imposta 2017" (parere 5 aprile 2018, n. 194, doc. web n. 8275691) che, rispetto a quanto previsto per gli anni di imposta precedenti, si limita ad introdurre per il contribuente, a partire dalla dichiarazione precompilata 2018, un'importante nuova funzionalità di compilazione agevolata, prima non prevista dal sistema, che consente di rettificare i dati delle spese sanitarie e veterinarie indicate nella dichiarazione precompilata attraverso la consultazione dei dati sul Sistema tessera sanitaria (Ts). Lo schema sottoposto all'attenzione del Garante ha tenuto conto delle indicazioni fornite dall'Ufficio ai rappresentanti del Mef, dell'Agenzia delle entrate e di Sogei s.p.a., volti a conformare ai principi in materia di protezione dei dati personali tale nuova funzionalità; ciò con particolare riferimento alle modalità tecniche di attuazione della stessa attraverso il Sistema Ts e alle modalità di consultazione dei dati rettificati dal contribuente da parte dell'Agenzia delle entrate, prevedendo che le informazioni di dettaglio rettificate possano essere visualizzate in relazione alle sole dichiarazioni sottoposte ad attività di controllo di cui al d.P.R. 29 settembre 1973, n. 600, attraverso l'applicativo dedicato ai controlli formali di cui all'art. 36-*ter* dello stesso.

Di conseguenza è stato trasmesso al Garante anche un nuovo schema di decreto del Ministro dell'economia e delle finanze concernente la predetta compilazione agevolata del quadro relativo agli oneri deducibili e detraibili della dichiarazione dei redditi, sul quale il Garante si è espresso favorevolmente (parere 26 aprile 2018, n. 248, doc. web n. 8641178). Lo schema di decreto, elaborato tenendo conto degli approfondimenti effettuati dall'Ufficio del Garante, oltre a disciplinare la nuova funzionalità di compilazione agevolata di rettifica dei dati trasmessi – attraverso la loro modifica, integrazione o cancellazione –, introduce una rilevante ulteriore funzionalità che consente ai contribuenti, dal 1° gennaio dell'anno di riferimento della spesa al 31 gennaio dell'anno successivo, di segnalare, attraverso il Sistema Ts, eventuali incongruenze al fine della correzione dei dati trasmessi. Particolare attenzione è stata posta dal Garante sulle modalità di realizzazione della predetta consultazione puntuale dei dati corretti dal contribuente da parte dei dipendenti dell'Agenzia delle entrate, sulle misure di sicurezza della nuova funzionalità di segnalazione delle

incongruenze agli erogatori di prestazioni sanitarie nonché sulle modalità di conservazione, da parte del Sistema Ts, in archivi distinti, dei dati trasmessi, comprensivi di quelli comunicati nell'ambito della compilazione agevolata da parte del contribuente, in modo che il codice fiscale dell'assistito sia separato da tutti gli altri dati.

Accesso dei Caf alla dichiarazione precompilata

Come negli anni precedenti, il Garante ha esaminato anche lo schema del nuovo provvedimento del Direttore dell'Agenzia sulle modalità di accesso alla dichiarazione precompilata da parte del contribuente e degli altri soggetti autorizzati che, nel confermare le modalità tecniche già sottoposte all'esame del Garante, prevede, a partire dal 2018, che i Centri di assistenza fiscale (Caf) e i professionisti abilitati possano effettuare richieste di accesso alle dichiarazioni precompilate via web, previa autenticazione, oltre che con le credenziali rilasciate dall'Agenzia delle entrate e con una Cns, anche con un'identità Spid. Alcuni Caf espressamente individuati possono inoltre accedere, in via sperimentale, in cooperazione applicativa con cornice di sicurezza, alle dichiarazioni dei redditi precompilate e alle informazioni attinenti alla dichiarazione 730 precompilata disponibili presso l'Agenzia delle entrate (parere 5 aprile 2018, n. 195, doc. web n. 8275939). Nel parere è dato atto che nello schema di provvedimento, in seguito a specifici approfondimenti effettuati con l'Ufficio, sono state individuate le misure di sicurezza necessarie per consentire ai Caf che aderiscono alla sperimentazione l'accesso alla precompilata, previa stipula di un'apposita convenzione con l'Agenzia delle entrate, redatta nel rispetto del provvedimento del Garante del 18 settembre 2008 (doc. web n. 1549548). Al riguardo, l'Autorità ha ritenuto necessario prescrivere ai predetti Caf l'adozione di una serie di misure al fine di ridurre al minimo i rischi di accessi non autorizzati o di trattamenti non consentiti ai dati personali oggetto di accesso. In particolare, i servizi di cooperazione applicativa resi disponibili dall'Agenzia delle entrate devono essere esclusivamente integrati dai Caf con il proprio sistema informativo e non possono essere resi disponibili a terzi, né direttamente né indirettamente, per via informatica. L'accesso ai servizi di cooperazione applicativa deve essere consentito esclusivamente dagli applicativi del Caf realizzati per le finalità di accesso alla dichiarazione precompilata e i servizi di cooperazione applicativa non possono essere utilizzati da soggetti esterni al Caf anche nell'ipotesi in cui questi operino per conto dello stesso. In nessun caso è consentita la messa a disposizione, da parte dei Caf, dei web service forniti su rete pubblica (Internet) e la procedura di autenticazione dell'utente deve essere protetta dal rischio di intercettazione delle credenziali da meccanismi crittografici di robustezza almeno equivalente a quella offerta dal protocollo TLS1.2 esclusivo, chiavi RSA 2048 bit e cifrari basati su algoritmo AES. I Caf devono altresì tracciare le operazioni concernenti la richiesta di accesso ai dati tramite il canale di cooperazione applicativa e conservarle secondo i requisiti di legge. Nelle richieste di accesso, oltre ai dati di riscontro richiesti per tutti gli accessi alla precompilata da parte dei soggetti autorizzati, devono essere indicati il codice *hash* del *file* in formato pdf contenente le copie della delega e del documento del contribuente delegante, nonché la modalità di sottoscrizione della delega. Oltre alle ordinarie modalità di controllo dell'Agenzia delle entrate sulle deleghe e sui documenti di identità indicati nelle richieste di accesso alle dichiarazioni precompilate, i Caf che aderiscono alla sperimentazione devono poi garantire anche un accesso, in cooperazione applicativa con cornice di sicurezza, ai predetti documenti indicati nelle richieste di accesso con modalità asincrona entro 48 ore dalla richiesta dell'Agenzia. Infine, i Caf devono utilizzare proprie procedure, di carattere organizzativo e tecnologico, in grado di evidenziare eventuali anomalie nelle attività di accesso ai dati da parte degli utilizzatori designati. A seguito di una

segnalazione prodotta dalle suddette procedure, i Caf dovranno adottare le opportune contromisure volte a prevenire accessi abusivi ai dati. Qualora non sia possibile adottare tempestivamente tali contromisure, i Caf dovranno procedere all'interruzione del servizio, dandone contestuale comunicazione all'Agenzia delle entrate.

In ogni caso, il Garante ha ritenuto necessario rinviare all'esito della valutazione condotta dall'Agenzia delle entrate, anche sulla base degli esiti dei controlli a campione effettuati durante la sperimentazione, il rafforzamento delle misure sopra individuate in relazione alle modalità di accesso dei Caf per i successivi anni d'imposta.

4.5.2. La fatturazione elettronica

Il Garante ha rilevato gravi criticità nelle modalità con le quali l'Agenzia delle entrate ha deciso di dare esecuzione al nuovo obbligo generalizzato di fatturazione elettronica introdotto dalla legge di bilancio 2018 (legge 27 dicembre 2017, n. 205), esteso, a partire dal 1° gennaio 2019, alle cessioni di beni e prestazioni di servizi effettuate tra due operatori Iva (operazioni *Business to Business*, cd. B2B), ma anche a quelle effettuate verso un consumatore finale (operazioni *Business to Consumer*, cd. B2C).

Come di seguito illustrato, l'Autorità è, pertanto, intervenuta nei confronti dell'Agenzia dell'entrate rappresentando la necessità di modificare le modalità di realizzazione della fatturazione elettronica atteso che la proporzionata raccolta di informazioni e i connessi rischi di usi impropri da parte di terzi potevano violare la normativa sulla protezione dei dati. Al fine di assicurare il giusto contemperamento tra le esigenze del fisco e i diritti e le libertà degli interessati, il Garante, su richiesta dell'Agenzia, ha poi ha avviato un tavolo di lavoro, in tempi assai ristretti, necessari a conformare i trattamenti al RGPD e al Codice prima dell'entrata in vigore del nuovo obbligo.

Avvertimento all'Agenzia delle entrate

Con un provvedimento adottato anche a seguito di alcuni reclami, il Garante ha esercitato per la prima volta il nuovo potere correttivo attribuito dal Regolamento europeo, avvertendo l'Agenzia delle entrate che le modalità con cui intendeva dare attuazione al nuovo obbligo generalizzato di fatturazione elettronica, esteso anche alle fatture tra operatori economici e consumatori, presentavano rilevanti criticità in ordine alla compatibilità con la normativa in materia di protezione dei dati personali.

Peraltro, i provvedimenti di attuazione di tale obbligo (provvedimenti del Direttore dell'Agenzia delle entrate nn. 89757 e 291241 del 30 aprile 2018 e del 5 novembre 2018) sono stati adottati senza consultare il Garante. Il tempestivo, oltre che necessario, coinvolgimento dell'Autorità, ora previsto anche in fase legislativa, avrebbe certamente potuto contribuire ad avviare il nuovo progetto con modalità e garanzie rispettose della protezione dei dati personali fin dalla progettazione. Per questo motivo è stato altresì richiesto all'Agenzia di far conoscere con urgenza le modalità individuate per rendere conformi al quadro normativo italiano ed europeo i trattamenti di dati che verranno effettuati ai fini della fatturazione elettronica (provv. 15 novembre 2018, n. 481, doc. web n. 9059949).

Entrando nel merito del nuovo sistema di fatturazione elettronica il Garante ha rilevato una serie di criticità in ordine alla compatibilità con la normativa in materia di protezione dei dati personali.

Principio di proporzionalità

In primo luogo, l'Agenzia, dopo aver recapitato le fatture in qualità di "postino" attraverso il sistema di interscambio (Sdi) tra gli operatori economici e i contribuenti (2,1 miliardi di fatture nel 2017), intende archiviare e utilizzare i dati anche

4

a fini di controllo. Tuttavia non sarebbero stati archiviati solo i dati obbligatori a fini fiscali, ma la fattura vera e propria, che contiene di per sé informazioni di dettaglio ulteriori sui beni e servizi acquistati, quali le abitudini e le tipologie di consumo, legate alla fornitura di servizi energetici e di telecomunicazioni (es. regolarità nei pagamenti, appartenenza a particolari categorie di utenti), o addirittura la descrizione delle prestazioni sanitarie o legali. Occorre poi considerare al riguardo che anche le fatture emesse nei confronti di una persona giuridica possono contenere dati riferiti a persone fisiche, come in caso di utenze telefoniche, biglietti ferroviari o aerei, pedaggi autostradali, pernottamenti.

Ulteriori criticità derivano dalla scelta dell'Agenzia delle entrate di mettere a disposizione sul proprio portale, senza una richiesta dei consumatori, in manifesto contrasto con il principio di *privacy by default*, oltreché di minimizzazione e di *privacy by design*, tutte le fatture in formato digitale, anche per chi preferirà comunque continuare a ricevere solo la fattura cartacea o digitale direttamente dal fornitore, come garantito dal legislatore, con un ingiustificato incremento dei rischi insiti in un trattamento massivo di dati accessibili tramite un applicativo web.

Il Garante ha, pertanto, rilevato, che il nuovo obbligo di fatturazione elettronica presenta un rischio elevato per i diritti e le libertà degli interessati, poiché comporta un trattamento sistematico, generalizzato e di dettaglio di dati personali su larga scala, potenzialmente relativo ad ogni aspetto della vita quotidiana dell'intera popolazione, sproporzionato rispetto all'obiettivo di interesse pubblico perseguito, pur legittimo, poiché tutte le fatture emesse contengono anche dati ulteriori rispetto a quelli obbligatori a fini fiscali.

Ruolo degli intermediari

Non è inoltre risultato chiaro il ruolo assunto dagli intermediari delegabili dal contribuente per la trasmissione, la ricezione e la conservazione delle fatture, alcuni dei quali operano anche nei confronti di una moltitudine di imprese, accentrando enormi masse di dati personali che non si riscontrano nella normale gestione delle attività economiche in cui, di regola, non vengono messe a disposizione di terzi informazioni sui beni e servizi ceduti, sulla clientela e sulle relative abitudini di consumo, con un aumento dei rischi, non solo per la sicurezza delle informazioni, ma anche relativi a ulteriori usi impropri, grazie a possibili collegamenti e raffronti tra fatture di migliaia di operatori economici.

Modalità di trasmissione delle fatture

Sono state rilevate ulteriori criticità che possono verosimilmente violare il RGPD in relazione ai profili di sicurezza, di correttezza e trasparenza del trattamento. In particolare, per quanto riguarda i canali di trasmissione e recapito delle fatture elettroniche, è stato ancora previsto l'uso il protocollo FTP, che non può essere considerato un canale sicuro ai sensi dell'art. 32 del RGPD. Un'ulteriore criticità deriva dalla mancata cifratura del *file* xml della fattura elettronica. Ciò considerando, in particolare, il previsto utilizzo della Pec per lo scambio delle fatture, con la conseguente possibile memorizzazione dei documenti sui *server* di gestione della posta elettronica, che espone gli interessati a maggiori rischi di accesso non autorizzato ai dati personali (utilizzo non esclusivo della Pec in ambito aziendale, furto di credenziali e attacchi informatici ai *server*).

Non sarebbero state inoltre correttamente rappresentate agli utenti nell'informativa le ulteriori finalità di conservazione e di controllo perseguite dall'Agenzia con i dati raccolti attraverso tale applicazione.

Per quanto riguarda, invece, il servizio gratuito di conservazione delle fatture offerto dall'Agenzia, non è stato ben chiarito il ruolo assunto in relazione al trattamento dei dati personali e alle conseguenti responsabilità.

Tavolo di lavoro

In seguito al menzionato provvedimento del 15 novembre 2018, n. 481, su richiesta dell'Agenzia, è stato costituito un tavolo di lavoro tecnico per esaminare

congiuntamente le criticità rilevate dal Garante, nell'ambito del quale, per gli aspetti di competenza, sono stati coinvolti anche il Mef, l'AgID, il Consiglio nazionale dei dottori commercialisti e degli esperti contabili, il Consiglio nazionale dell'ordine dei consulenti del lavoro e l'associazione dei produttori di *software* gestionale e fiscale (AssoSoftware).

All'esito di tale tavolo di lavoro, con un articolato provvedimento, il Garante – preso atto delle modifiche apportate all'impianto normativo originario della fatturazione elettronica e delle ulteriori rassicurazioni fornite dall'Agenzia delle entrate – ha individuato i presupposti e le condizioni perché la stessa Agenzia potesse avviare dal 1° gennaio 2019 i trattamenti di dati connessi al nuovo obbligo (provv. 20 dicembre 2018, n. 511, doc. web n. 9069072).

In tale provvedimento, di seguito sintetizzato, il Garante ha esaminato i trattamenti a rischio elevato effettuati nell'ambito della fatturazione elettronica, anche ai sensi dell'art. 36, par. 5, del RGPD e dell'art. 2-*quinquesdecies* del Codice, e si è espresso sulle modifiche apportate dall'Agenzia ai relativi provvedimenti attuativi.

In primo luogo, è stato reputato sproporzionato, rispetto alle finalità perseguite, l'impianto originario della fatturazione elettronica prefigurato dell'Agenzia, che aveva ritenuto di procedere alla memorizzazione integrale – in formato xml – di tutte le fatture, emesse e ricevute, comprensive dei relativi allegati, contenenti anche dati personali ulteriori rispetto a quelli obbligatori a fini fiscali; ciò avuto riguardo anche ai rischi elevati per i diritti e le libertà degli interessati che un simile trattamento inevitabilmente determina. La sproporzione è stata eccepita dal Garante non solo per i dati non rilevanti a fini fiscali, riportati dagli operatori economici nelle fatture e negli allegati, ma anche per le informazioni obbligatorie ai sensi dell'art. 21, d.P.R. 29 settembre 1973, n. 600, quali quelle relative alla descrizione del bene o del servizio oggetto di fatturazione (natura, qualità e quantità del bene ceduto o del servizio reso). Particolari criticità presenta poi il trattamento delle fatture emesse da operatori attivi in ambito sanitario e dagli avvocati, che riportano, nella descrizione, informazioni specifiche sulle prestazioni eseguite riferibili anche a patologie o a puntuali vicende giudiziarie, con il trattamento di particolari categorie di dati e di dati relativi a condanne penali e reati (artt. 9 e 10 del RGPD).

Al fine di conformare il trattamento al RGPD, nel tavolo di lavoro si è reso necessario anzitutto individuare puntualmente le finalità perseguite dall'Agenzia nell'esecuzione dei compiti di interesse pubblico affidatile dal legislatore, individuando, per ciascuna, i correttivi necessari.

a) Recapito delle fatture attraverso lo Sdi a operatori economici e consumatori. L'integrale memorizzazione del *file* xml e dei relativi allegati risulta indubbiamente necessaria al fine di recapitare la fattura elettronica attraverso il Sistema d'interscambio (Sdi) mediante il canale (cd. indirizzo telematico) prescelto dai contribuenti. Il Garante ha tuttavia rilevato che tale trattamento deve avvenire nel più rigoroso rispetto dei principi di minimizzazione, integrità e riservatezza, con l'adozione di adeguate misure tecniche e organizzative a cura di tutti i soggetti coinvolti nella filiera della fatturazione elettronica (operatori economici, intermediari, altri soggetti delegati e Agenzia delle entrate).

b) Servizio di consultazione delle fatture per gli operatori economici e i consumatori. L'Autorità ha ritenuto tale trattamento proporzionato e conforme al RGPD solo se espressamente richiesto ed effettuato in nome e per conto degli operatori economici. La finalità perseguita attraverso una generalizzata messa a disposizione di tutti i contribuenti di tale servizio, anche in assenza di una loro specifica richiesta, non può giustificare, infatti, per impostazione predefinita, una complessiva e integrale archiviazione da parte dell'Agenzia delle entrate di miliardi di fatture; soprat-

tutto considerato che i consumatori hanno sempre il diritto di ottenere sempre una copia della fattura, digitale o analogica, direttamente dall'operatore valida a fini fiscali. Il servizio di consultazione deve pertanto essere messo a disposizione dall'Agenzia agli operatori economici in base di uno specifico accordo che, nell'ambito delle proprie scelte organizzative, volessero avvalersi a tal fine dell'Agenzia delle entrate, ai sensi dell'art. 28 del RGPD, in qualità di responsabile del trattamento dei dati personali relativi a terzi contenuti nelle fatture. Analogamente, anche i consumatori che volessero utilizzare tale servizio dovrebbero stipulare un apposito accordo, base giuridica per il trattamento da parte dell'Agenzia ai sensi dell'art. 6, par. 1, lett. *b*), del RGPD. In assenza dell'adesione ai predetti servizi, l'Agenzia memorizzerà il *file* xml della fattura nei soli casi residuali in cui la messa a disposizione della fattura nell'area riservata del portale dell'Agenzia sia una delle modalità previste per la consegna della stessa al destinatario, ovvero quando, per cause tecniche, il recapito non fosse possibile. L'Autorità ha ingiunto, in ogni caso, all'Agenzia di trasmettere, appena predisposti, i modelli di accordi di adesione al servizio di consultazione e *download* delle fatture, al fine di verificarne la conformità al RGPD.

c) Controlli fiscali automatizzati e puntuali. Nell'ottica della protezione dei dati personali, le attività di controllo fiscale effettuate dall'Agenzia possono essere ricondotte a due tipologie: la prima basata su trattamenti automatizzati (ad es., quelli volti a rilevare le incongruenze tra i dati dichiarati e quelli a disposizione dell'Agenzia nonché quelli relativi all'analisi del rischio evasione) e l'altra, più analitica, fondata sull'esame puntuale della posizione fiscale del contribuente e della documentazione fiscale nell'ambito di accertamenti fiscali e verifiche, anche da parte della Guardia di finanza. I controlli automatizzati richiedono, per loro natura, la memorizzazione e l'elaborazione massiva dei dati estratti dalle fatture (cd. dati fattura), utilizzati anche per finalità di assistenza, controllo finalizzato all'erogazione dei rimborsi Iva e predisposizione della dichiarazione dei redditi e dell'Iva, e messi anche a disposizione del contribuente sul portale dell'Agenzia per rilevare le incongruenze con i versamenti Iva. In ossequio al principio di minimizzazione, il Garante ha ritenuto sproporzionato far ricadere, tra i dati utilizzabili per i controlli automatizzati, il campo della fattura contenente la descrizione dell'operazione che, oltre a contenere dati di dettaglio sopra esemplificati, relativi alla natura, qualità e quantità dei beni e dei servizi fatturati, e presentare quindi rischi elevati per gli interessati, non si presta ad elaborazioni massive, poiché richiede un esame puntuale, caso per caso, del contenuto. L'Agenzia ha quindi proposto al Garante, di non memorizzare i dati contenuti nei campi relativi alle "descrizioni" (compresi quelli attinenti ai codici "parlanti"), contenenti dati personali di dettaglio e più delicati. Una volta consegnata la fattura, devono essere, pertanto, memorizzati unicamente i dati fattura necessari ai controlli automatizzati e quelli necessari a garantire il processo di fatturazione (compreso il codice *hash* del *file* xml, codice alfanumerico necessario a verificarne l'autenticità e l'integrità del documento esibito in sede di controllo), mentre i dati "non fiscali", unitamente al dato fiscale relativo alla descrizione dell'operazione, saranno cancellati. Al riguardo, tuttavia, il Garante ha invitato l'Agenzia a rivalutare anche la memorizzazione di alcuni campi relativi ai "dati trasporto" che deve risultare adeguata, pertinente e limitata rispetto alla finalità per le quali tali dati devono essere trattati. Più in generale, con riferimento ai trattamenti automatizzati a fini di controllo, il Garante ha ricordato all'Agenzia che, oltre agli specifici obblighi di trasparenza del trattamento nei confronti degli interessati, il nuovo quadro giuridico prevede precise garanzie e adempimenti in relazione ai trattamenti automatizzati di dati personali che presentano rischi elevati per i diritti e le libertà degli interessati di cui occorre tenere

conto. L'archiviazione generalizzata delle fatture è risultata sproporzionata anche per l'esecuzione dei controlli puntuali, risultati molto limitati rispetto alla generale platea di contribuenti alla luce dei dati quantitativi di accertamenti fiscali e verifiche effettuati negli anni passati forniti dall'Agenzia. L'introduzione della fattura elettronica potrà invece agevolare i controlli a distanza, con nuove modalità di acquisizione delle fatture da parte dell'Agenzia, anche in relazione alle fatture per le quali il contribuente ha aderito al servizio di consultazione e *download* delle fatture.

d) Servizio di conservazione delle fatture. L'Agenzia ha perfezionato nell'ambito del tavolo di lavoro l'accordo in base al quale, a richiesta, mette a disposizione dei contribuenti, in qualità di responsabile del trattamento dei dati, tramite Sogei s.p.a., un servizio di conservazione delle fatture. Il Garante ha convenuto che, per realizzare il nuovo impianto della fatturazione elettronica conforme al RGPD, l'Agenzia necessiti, di un periodo transitorio, che decorre dal 1° gennaio 2019 fino al 2 luglio 2019, per realizzare l'acquisizione dei dati fattura e il servizio di consultazione, in cui il trattamento sarà limitato alla sola memorizzazione dei dati fattura per la consultazione e *download* dei *file* xml, evitando qualunque altro utilizzo.

Le fatture elettroniche emesse dai soggetti che erogano prestazioni sanitarie

Il Garante ha valutato con favore il temporaneo regime derogatorio introdotto dal legislatore in ambito sanitario che ha esonerato dalla fatturazione elettronica i soggetti tenuti all'invio dei dati al sistema Tessera sanitaria (Ts), per il periodo di imposta 2019, con riferimento alle fatture i cui dati sono inviati al predetto Sistema.

Tuttavia l'Autorità ha rilevato che tale esonero *ex lege* non opera nei confronti delle fatture emesse dai soggetti che erogano prestazioni sanitarie non trasmesse attraverso il Sistema Ts, ad esempio in seguito all'opposizione legittimamente manifestata dagli interessati e quindi, paradossalmente, proprio per le situazioni ragionevolmente più delicate. Inoltre, negli operatori sanitari permaneva il dubbio se l'eventuale emissione di una fattura elettronica attraverso lo Sdi, nonostante il predetto esonero, fosse conforme al RGPD.

Al riguardo, il Garante ha chiarito nel provvedimento che, alla luce del quadro normativo vigente, l'utilizzo del sistema di fatturazione elettronica da parte del professionista non potrebbe essere ritenuto lecito, ai sensi dell'art. 6, par. 1, lett. *c*), del RGPD, essendo stato espressamente esonerato dall'obbligo di emissione della fattura elettronica in caso di trasmissione dei relativi dati attraverso il Sistema Ts.

È stato pertanto ingiunto all'Agenzia delle entrate di dare idonee istruzioni a tali soggetti affinché in nessun caso sia emessa una fattura elettronica attraverso lo SDI concernente l'erogazione di una prestazione sanitaria, a prescindere dall'invio dei dati attraverso il Sistema Ts, in modo da evitare trattamenti di dati in violazione del Regolamento e del Codice da parte dell'Agenzia stessa e di tutti i soggetti a vario titolo coinvolti nel processo di fatturazione elettronica.

La sicurezza del trattamento

Nel tavolo di lavoro, con riferimento alla mancata adozione di misure di protezione crittografica dei *file* xml delle fatture elettroniche, l'Agenzia ha rappresentato che l'applicazione di algoritmi di cifratura (anche parziali), sia simmetrici che asimmetrici, non risulterebbe compatibile con un modello in cui la fattura deve essere leggibile dal cedente/prestatore, dal cessionario/committente, dagli eventuali soggetti delegati alla gestione delle fatture nonché, ai fini dell'estrazione dei dati fattura, dall'Agenzia delle entrate.

Al riguardo, il Garante ha rilevato che spetta al titolare del trattamento individuare le misure tecniche e organizzative adeguate per garantire la protezione dei dati anche con tecniche crittografiche, nel rispetto dei principi di *privacy by design* e *by default*, attraverso un'attenta analisi dei processi e un adeguato impegno progettuale. In questo ambito, tecniche di cifratura e scambio di messaggi tra più soggetti sono

4

da tempo disponibili e potrebbero essere implementate, anche gradualmente, tenendo conto dell'impatto della cifratura sulle prestazioni complessive e sull'usabilità dei servizi informatici a supporto del processo di fatturazione elettronica. Pertanto, alla luce di tali considerazioni, l'Agenzia delle entrate è stata invitata a fornire entro il 15 aprile 2018 una nuova analisi di tali aspetti, anche nell'ambito della valutazione di impatto.

Ulteriori approfondimenti sono stati richiesti all'Agenzia anche in relazione all'utilizzo della Pec, quale canale di trasmissione e ricezione delle fatture, atteso che le menzionate tecniche di cifratura consentirebbero di eliminare i rischi ivi prospettati. L'Agenzia è stata altresì invitata a illustrare, nelle istruzioni fornite ai contribuenti, i rischi insiti in tale canale di trasmissione e recapito delle fatture, soprattutto laddove i *file* xml non vengano cancellati dai *server* di posta ovvero vengano utilizzate caselle Pec a uso non esclusivo dell'interessato.

La valutazione di impatto sulla protezione dei dati

Il Garante ha rilevato, in generale, che una valutazione di impatto dovrebbe in primo luogo tenere conto dei rischi incombenti sui diritti e sulle libertà degli interessati, esaminando, in modo esaustivo, i diversi scenari di rischio e i possibili impatti al fine di individuare misure adeguate ad affrontarli, annullandoli o, quantomeno, riducendoli a un livello accettabile.

La valutazione di impatto effettuata dall'Agenzia è risultata, invece, focalizzata su aspetti meramente tecnici del trattamento, traducendosi prevalentemente, se non esclusivamente, in un documento di valutazione del rischio informatico incombente sui dati, carente nella parte analitica riferita agli impatti sui diritti e sulle libertà degli interessati derivanti dai diversi scenari di rischio considerati, anche laddove non siano riferibili alla fattispecie degli incidenti informatici.

Pur considerando la recente introduzione di tale adempimento, la complessità e la portata della fatturazione elettronica, che coinvolge l'intera popolazione, richiedono che la valutazione di impatto sia realizzata evitando di sfruttare schemi standard e semplificazioni che rischiano di comprometterne l'efficacia, fornendo alla stessa un connotato di eccessiva genericità e di inadeguatezza, soprattutto in relazione all'analisi dei rischi che ne costituisce il presupposto essenziale.

Inoltre, non è risultato che, come previsto dall'art. 35, par. 9, del RGPD, l'Agenzia abbia raccolto, attraverso le modalità ritenute più opportune, e tenuto in considerazione nell'ambito della valutazione di impatto, le opinioni degli interessati o dei loro rappresentanti, quali le associazioni di categoria o di consumatori. Anche quando avesse ritenuto non appropriato procedere in tal senso, avrebbe dovuto quantomeno documentare, all'interno del documento, i motivi della mancata raccolta delle opinioni degli interessati.

Il Garante ha, pertanto, ingiunto all'Agenzia delle entrate di comunicare, entro il 15 aprile 2019, una nuova versione della valutazione di impatto, riesaminando gli elevati rischi connessi al processo di fatturazione elettronica, anche alla luce di quanto emergerà nei primi mesi di operatività del nuovo obbligo.

Intermediari e altri soggetti operanti nell'ambito della fatturazione elettronica

Il Garante ha evidenziato che gli operatori economici devono prestare particolari cautele in ordine all'articolato sistema di deleghe delineato dall'Agenzia, soprattutto in considerazione dei rischi connessi al trattamento dei personali di terzi coinvolti nel processo di fatturazione.

Gli intermediari e gli altri soggetti delegati assumono, in tale contesto, il ruolo di responsabile o sub-responsabili del trattamento, a seconda delle scelte organizzative degli operatori economici e dei relativi modelli contrattuali utilizzati.

Il Garante ha formulato alcuni rilievi critici in relazione ad alcuni modelli contrattuali utilizzati dalle maggiori società produttrici di *software* gestionale e fiscale, che evidenziano elevati rischi di utilizzi impropri dei dati personali nell'ambito dei

trattamenti effettuati dagli intermediari e dagli altri soggetti delegati dagli operatori economici nel processo di fatturazione.

Non è risultata infatti conforme al RGPD la clausola in cui è previsto che una società produttrice di *software* gestionale e fiscale possa autonomamente procedere all'elaborazione e all'utilizzo di informazioni, su base aggregata e previa anonimizzazione, ivi incluse informazioni relative ai meta-dati associati alle fatture, a fini di studio e statistici, attraverso una licenza non esclusiva, perpetua, irrevocabile, valida in tutto il mondo e a titolo gratuito, ad utilizzare tali informazioni per dette finalità. I dati personali contenuti nelle fatture, infatti, non sono riferiti esclusivamente all'operatore economico che le ha emesse e ricevute, ma pure ai terzi – anche persone fisiche – con cui intrattiene rapporti economici. I trattamenti svolti in qualità di responsabile e di sub-responsabile devono, pertanto, essere limitati solo ed esclusivamente a quanto necessario per la fornitura dei servizi forniti al titolare e, dunque, per l'esecuzione del contratto stesso, senza introdurre operazioni di trattamento ulteriori (ivi compresa l'anonimizzazione dei dati) preordinate al perseguimento di finalità proprie del responsabile, rispetto alle quali deve essere, di volta in volta, valutata la rispondenza ai requisiti del RGPD, quali, in particolare, i presupposti di liceità del trattamento e il rispetto dei principi applicabili al trattamento dei dati personali.

Sono state rilevate altresì peculiari modalità di articolazione dei ruoli assunti nel trattamento dei dati personali oggetto della fatturazione elettronica, che non ripartiscono correttamente le responsabilità circa i rischi derivanti dal trattamento, introducendo sproporzionati esoneri di responsabilità, soprattutto in caso di contratti standard, con margini di negoziazione pressoché nulli in capo al titolare del trattamento.

Più in generale, il Garante ha richiamato, infine, l'attenzione sulle modalità con cui viene attuato l'obbligo di autorizzazione scritta all'utilizzo di altri responsabili da parte dell'iniziale responsabile del trattamento, con situazioni che, in concreto, in violazione del principio di *accountability*, potrebbero privare il titolare di strumenti di controllo delle attività di trattamento effettuate sotto la propria responsabilità.

Pertanto, l'Autorità, in relazione a tali aspetti, ha avvertito gli operatori economici, gli intermediari e gli altri soggetti delegati che trattamenti effettuati in base alle clausole contrattuali analoghe possono violare gli artt. 5, 6 e 28 del RGPD.

4.5.3. Riscossione a mezzo ruolo

Nel corso del 2017 l'Agenzia delle entrate ha chiesto di consentire all'Agenzia delle entrate - Riscossione, di accedere, per la riscossione mediante ruolo, oltre che alle informazioni circa l'esistenza di rapporti finanziari, anche a quelle relative alle consistenze degli stessi (cd. dati contabili, quali ad es. saldi e giacenza media) presenti nell'Archivio dei rapporti finanziari. L'accesso a tali informazioni agevola, infatti, un'attività di riscossione mirata e più efficiente, nonché meno invasiva nei confronti del contribuente sul quale non graverà più il rischio di indisponibilità di tutti i rapporti finanziari, intrattenuti anche con più operatori, a prescindere dalla presenza su un singolo rapporto della somma sufficiente ad estinguere il debito. Saranno così anche evitati gli interscambi dati puntuali tra l'Agenzia delle entrate - Riscossione con i singoli operatori finanziari riguardanti rapporti i cui dati contabili lasciano trasparire una palese inefficacia dell'azione esecutiva.

Il Garante non ha ritenuto sufficienti ad attenuare i rischi elevati di tale trattamento le misure inizialmente individuate dall'Agenzia ed è stata quindi avviata un'approfondita interlocuzione volta a valutare l'introduzione di ulteriori accorgimenti, sia con riferimento alle modalità di accesso all'archivio dei rapporti finan-

ziari, che al loro successivo trattamento, nell'ambito delle procedure di riscossione a mezzo ruolo.

A conclusione dell'istruttoria, il Garante ha ritenuto, anche sulla base delle indicazioni fornite nelle numerose interlocuzioni, siano state individuate misure idonee a ridurre i rischi a un livello accettabile in relazione, in particolare, alle modalità di accesso, consentito solo in presenza della corretta associazione tra il codice fiscale del debitore e il numero di ruolo, al sistema di autorizzazioni articolato su due livelli, ai controlli sugli accessi, alle modalità di trattamento da parte dell'Agenzia delle entrate - Riscossione con misure di sicurezza anche organizzative, quali l'utilizzo di PDF non ricercabili, il divieto di duplicazione dei dati e la cancellazione automatica/tempestiva dei dati, nonché alla gradualità dei dati contabili delle procedure esecutive (nota 22 giugno 2018).

4.5.4. Soluzioni per il sistema economico - Sose s.p.a.

È stato predisposto altresì il parere favorevole sullo schema di "Convenzione Quadro tra il Mef e la Soluzioni per il sistema economico – Sose s.p.a." avente ad oggetto l'affidamento a tale società di alcuni servizi e attività da svolgere in favore dell'amministrazione finanziaria, tra cui l'elaborazione di indici sintetici di affidabilità (Isa), nonché ogni altra attività di studio e ricerca in materia tributaria, la definizione di metodologie per la determinazione dei fabbisogni standard e capacità fiscali standard delle regioni a statuto ordinario e lo svolgimento delle attività necessarie per l'attuazione del federalismo fiscale. La versione dello schema di convenzione ha tenuto conto delle indicazioni fornite dall'Ufficio nel corso dell'istruttoria, volte ad assicurare la conformità alle indicazioni a suo tempo fornite dal Garante nel parere del 2001 sulla precedente convenzione quadro e anche al RGPD, con particolare riferimento alla corretta individuazione del ruolo assunto da Sose in relazione al trattamento dei dati personali, prevedendo la designazione quale responsabile del trattamento nell'ambito di un contratto o altro atto giuridico da allegare a ciascun atto esecutivo della convenzione quadro, in conformità all'art. 28 del RGPD, alla necessità di individuare, negli atti esecutivi della convenzione, attraverso istruzioni documentate del titolare del trattamento, le specifiche categorie di interessati e di dati messi a disposizione da Sose, per l'espletamento degli incarichi affidati, nonché le relative modalità di minimizzazione degli stessi, nel rispetto dei principi di esattezza, di limitazione della finalità e della conservazione, di integrità e riservatezza, nonché alla limitazione del trattamento dei dati effettuato da Sose che potrà utilizzare, esclusivamente dati e informazioni che le strutture organizzative raccolgono e detengono in base a specifiche disposizioni normative, mentre ulteriori informazioni potranno essere acquisite direttamente solo su indicazione delle strutture organizzative titolari del trattamento, previa esatta individuazione delle categorie di interessati e delle categorie di dati personali trattati (provv. 26 luglio 2018, n. 439, doc. web n. 9027442).

4.6. *Verifiche relative alle procedure di rilascio dei visti e al trasferimento dei dati nel Sistema di informazione visti*

Nell'ambito degli specifici obblighi di vigilanza previsti dall'art. 41 del regolamento (CE) n. 767/2008 – in base al quale le autorità di controllo nazionali esercitano autonomamente i poteri di verifica sulla legittimità del trattamento dei dati personali registrati nel Sistema informativo visti, *Visa Information System* (VIS; art. 41, par. 1) e svolgono, almeno ogni quattro anni, un'attività di controllo sulle operazioni

4

di trattamento dei dati del sistema nazionale –, il Garante, in qualità di autorità competente per la supervisione nazionale del Sistema informativo Schengen II e di Sistema informativo visti, ha concluso nel 2018 il ciclo di controlli avviati nel 2016.

Tale attività, come riferito nella precedente Relazione (p. 80), era stata oggetto di una specifica raccomandazione all'esito della valutazione Schengen (Sche-Eval), conclusa nel 2016, relativa all'applicazione dell'*Acquis* di Schengen nel settore della protezione dei dati personali da parte dell'Italia, effettuata dal gruppo di valutazione formato da esperti designati delle autorità di protezione dati dei Paesi Schengen e coordinato da rappresentanti della Commissione europea che ha redatto il previsto rapporto secondo la procedura prevista dal regolamento (UE) 1053/2013.

L'attività di verifica ha riguardato la legittimità del trattamento dei dati personali effettuati dal Ministero degli affari esteri e della cooperazione internazionale nelle procedure di rilascio dei visti e nel trasferimento dei dati nel Sistema di informazione visti (*Visa Information System*, VIS, istituito con la decisione del Consiglio dell'Unione Europea 2004/512/CE del 8 giugno 2004 e disciplinato dal regolamento (CE) n. 767/2008 e dalla decisione del Consiglio 2008/633/HA del 23 giugno 2008) finalizzato allo scambio dei dati relativi ai visti d'ingresso Schengen. La complessa attività di controllo ha compreso, tra l'altro, attività ispettive presso la sede del Ministero nonché presso una sede consolare all'estero, in occasione della quale è stata anche visitata una delle sedi operative di una società esterna che fornisce in *outsourcing* servizi per i visti (*Esternal Services Provider*, ESP), e un *audit* di tipo documentale – volto a verificare il rispetto dei requisiti di sicurezza indicati nelle normative tecniche ISO 27001:2013 e ISO 27002:2013 e delle impostazioni "*privacy by design/by default*" –, le cui risultanze hanno fornito lo spunto per ulteriori approfondimenti di natura tecnologica, organizzativa e procedurale come pure per l'individuazione di alcune aree di miglioramento.

Le attività ispettive hanno avuto ad oggetto il funzionamento del sistema nazionale N-Vis, del sistema L-Vis (in uso presso i consolati) e del cd. Visa-Out (l'interfaccia utilizzata dai fornitori esterni di servizi per l'inserimento dei dati dei richiedenti il visto), in relazione ai soggetti abilitati all'accesso a tali sistemi, alle modalità di accesso, consultazione e inserimento dei dati e ai termini di conservazione. Sono state esaminate le procedure di rilascio dei visti – la gestione telematica e cartacea delle pratiche – in relazione alle modalità di adempimento delle garanzie in materia di protezione dei dati personali (informativa, esercizio dei diritti), anche con riguardo alle fasi della procedura espletate presso gli sportelli dell'*outsourcer*. Le criticità rilevate hanno riguardato i tempi di conservazione dei dati in N-VIS, le modalità e i tempi di conservazione dei dati in Visa-Out, la disponibilità dei dati dei richiedenti i visti nei sistemi informativi dell'*outsourcer*, le modalità di consegna delle credenziali agli operatori dell'*outsourcer*, la gestione e analisi dei *file* di *log* degli accessi al N-VIS, L-VIS e Visa-Out, sia presso il Ministero che presso gli uffici visti.

All'esito del complesso di attività sopra descritte, in relazione ai profili di criticità rilevati, il Garante ha adottato un provvedimento con il quale sono state indicate una serie di misure da adottare per elevare le garanzie relative al trattamento dei dati relativi ai richiedenti il visto (provv. 19 luglio 2018, n. 425, doc. web n. 9040249).

4.7. *I trattamenti effettuati presso regioni ed enti locali*

"Scuse" *online*

È stata conclusa una istruttoria nei confronti del Corpo di polizia locale di un comune di grandi dimensioni in relazione alle prescelte modalità di riparazione del danno derivante dal reato di oltraggio al pubblico ufficiale. In luogo del risarci-

mento pecuniario del pregiudizio, il citato Corpo di polizia aveva previsto una forma di ristoro (per dir così) "per equivalente", consistente nella pubblicazione su internet di un video di scuse da parte dell'autore della condotta, riservandosi di pubblicare, altresì, sui propri profili *social network*, notizie contenenti il riferimento al *link* Url dei video pubblicati. Il Garante ha ritenuto tali modalità, *in thesi* riparatorie del danno derivante dal reato ex art. 341-*bis* c.p., non conformi alla disciplina vigente (artt. 21 e 22, d.lgs. n. 196/2003), invitando il Corpo di polizia locale a una scelta rispettosa della dignità della persona e conforme al quadro normativo vigente in materia di protezione dei dati personali (nota 25 maggio 2018).

Consultazione *online* della cittadinanza

L'Autorità è stata interpellata da un comune di grandi dimensioni in relazione alle modalità di selezione e di partecipazione ad una iniziativa di consultazione *online* dei cittadini per il bilancio partecipativo. Al riguardo, l'ente ha rappresentato che, tra le azioni prioritarie del programma di governo, prevede quella di "garantire la partecipazione di cittadini ai processi decisionali con strumenti di democrazia partecipata e diretta" e che, con propria delibera, devono essere regolamentate le modalità di partecipazione e di selezione di un campione di cittadini, residenti o domiciliati nei municipi interessati che, su base volontaria, prendano parte alla discussione di idee o proposte progettuali da finanziare con le risorse individuate con precedente delibera.

Al riguardo, è stato richiesto al Garante se il trattamento dei dati personali connessi all'iniziativa in esame possa essere effettuato senza il consenso degli interessati "costituendo ai sensi dell'art. 6, lett. *e*), del RGPD, un trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare", oppure se, per converso, lo stesso sia subordinato alla preventiva acquisizione del consenso. Evidenziando che gli strumenti di partecipazione e consultazione rientrano tra quelli disciplinati dallo Statuto dell'ente locale (iniziativa popolare e istituti di partecipazione), l'Ente ha precisato che tale atto favorisce l'uso delle nuove tecnologie per promuovere una maggiore partecipazione della comunità cittadina al processo democratico, anche nelle questioni riguardanti l'utilizzo e la destinazione delle risorse economiche attraverso il bilancio partecipativo. Tali forme di consultazione, per lo Statuto, possono essere attuate anche con il ricorso a tecnologie informatiche e telematiche; con specifico riferimento alla consultazione sul bilancio partecipato, è previsto che la stessa avvenga, previa selezione casuale dei partecipanti (tra i residenti appartenenti al municipio interessato) con la successiva sottoposizione a consultazione finale *online* mediante strumenti informatici e telematici, delle proposte organizzate dai partecipanti precedentemente selezionati su base volontaria.

L'Ufficio ha ritenuto condivisibile l'ascrizione dei trattamenti dei dati in esame tra quelli disciplinati all'art. 6, par. 1, lett. *e*), del RGPD, necessari "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento", per i quali non è necessario richiedere il consenso degli interessati. Ha tuttavia precisato che il requisito di liceità sopra richiamato è condizionato al puntuale rispetto del quadro normativo che disciplina il trattamento, anche sotto il profilo delle fonti. Sono state pertanto richiamate le disposizioni statutarie che prevedono che siano disciplinati con gli atti di natura regolamentare ivi previsti i "modi e i limiti" degli "istituti di partecipazione e di iniziativa popolare", i "criteri e le modalità di informazione e consultazione e partecipazione, anche mediante strumenti informatici e telematici, dei cittadini al bilancio partecipativo", le modalità di svolgimento delle altre forme di consultazione, "anche con il ricorso a tecnologie informatiche e telematiche".

È stata infine richiamata l'attenzione sulla necessità che i trattamenti siano

conformi ai principi previsti dall'art. 5 del RGPD – liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, limitazione della conservazione – con particolare riferimento al principio di integrità e riservatezza (art. 5, par. 1, lett. *f*), delle disposizioni in materia di sicurezza del trattamento (art. 32) e di valutazione di impatto (art. 35) e, al fine di evitare il verificarsi di criticità analoghe a quelle rilevate in relazione ad altre consultazioni effettuate con l'utilizzo di piattaforme telematiche di partecipazione pubblica, sono stati richiamati anche i recenti provvedimenti adottati dall'Autorità sul tema (provv.ti 21 dicembre 2017, n. 548, doc. web n. 7400401; 16 maggio 2018, n. 289, doc. web n. 8999795; nota 31 maggio 2018).

Raccolta differenziata

Interpellato da numerosi comuni e singoli interessati, il Garante è intervenuto nuovamente in relazione agli aspetti di protezione dei dati personali connessi alla attività di raccolta differenziata svolta dagli enti locali. Pur riconoscendo la legittimità di salvaguardare il rispetto della disciplina sulla raccolta differenziata anche alla luce delle attuali e diffuse problematiche ambientali, il Garante ha ribadito la necessità di tutelare il diritto degli interessati a non subire violazioni ingiustificate della propria sfera di riservatezza, considerato che tra i rifiuti possono confluire, in particolare, effetti personali che sono talvolta relativi ad informazioni concernenti la sfera della salute o politico-religioso-sindacale. Per tali ragioni, anche nell'ottica del principio di responsabilità di cui all'art. 24 del RGPD, il Garante ha invitato numerosi comuni a valutare la conformità delle prescelte modalità di raccolta differenziata al quadro normativo vigente in materia di protezione dei dati personali (tra le tante, cfr. note 10 settembre 2018 e 26 marzo 2018).

Diritto d'accesso dei consiglieri comunali e provinciali

Con riferimento alla segnalazione di un cittadino, che lamentava che un documento del segnalante (segnatamente una dichiarazione di inizio attività - Dia), precedentemente richiesto dalla controparte nell'ambito di un procedimento di accesso ai sensi della legge n. 241/1990 conclusosi con diniego, era stato successivamente comunque prodotto in giudizio, l'Ufficio ha accertato che tale documento era stato consegnato alla controparte del segnalante da un consigliere comunale, che l'aveva acquisito dal comune ai sensi dell'art. 43, d.lgs. n. 267/2000. Tale disposizione prevede che i consiglieri comunali e provinciali hanno il "diritto di ottenere dagli uffici, rispettivamente, del comune e della provincia, nonché dalle loro aziende ed enti dipendenti, tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato" (art. 43, d.lgs. n. 267/2000), ferma restando la necessità che i dati personali così acquisiti siano utilizzati effettivamente per le sole finalità realmente pertinenti al mandato e non nell'interesse personale o di terzi. La normativa in materia di accesso ai documenti amministrativi, in caso di diniego espresso o tacito, individua specifici strumenti di tutela che l'istante può esercitare avanti alle autorità competenti (difensore civico, tribunale amministrativo regionale). Esulano dall'ambito di competenza dei consiglieri comunali le valutazioni in ordine alla liceità o meno delle determinazioni adottate dall'amministrazione sull'istanza, che sono sindacabili, invece, avanti alle predette autorità. Non è stato pertanto ritenuto riconducibile al suo *munus* l'operato del consigliere che, ritenuto illegittimo il diniego del comune, ha consegnato a quest'ultimo la documentazione dopo averla acquisita ai sensi dell'art. 43, d.lgs. n. 267/1990. Come costantemente ribadito infatti dalla giurisprudenza, la finalizzazione dell'accesso all'espletamento del mandato costituisce, al tempo stesso, il presupposto che legittima l'accesso ma anche il suo limite, ferma restando, pertanto, la necessità che i dati personali così acquisiti siano utilizzati effettivamente per le sole finalità realmente pertinenti al mandato, e non nell'interesse personale o di terzi, come nel caso in esame. Considerato che le risultanze istruttorie non hanno evidenziato una valida base normativa per la comunicazione dei dati contenuti nel documento in esame, la condotta del consigliere è

stata ritenuta in violazione degli artt. 11, comma 1, lett. *a*) e *b*), e 19, comma 3, d.lgs. n. 196/2003, l'Ufficio si è riservato di valutare, con autonomo procedimento, la sussistenza dei presupposti per l'applicazione di eventuali sanzioni (nota 17 maggio 2018).

4.8. *La previdenza e l'assistenza sociale*

Profilazione dei lavoratori assenti per malattia

A seguito di alcune notizie di stampa sono stati avviati opportuni accertamenti sul trattamento di dati personali, anche idonei a rivelare lo stato di salute, effettuato dall'Inps mediante un *software* finalizzato a rendere più efficienti i controlli sulle assenze dei lavoratori in ambito privato. Attraverso tale trattamento, analizzando, in particolare, frequenza e durata delle malattie, il *software* era in grado di profilare gli interessati attribuendo un "punteggio" volto ad individuare immediatamente i certificati più a rischio per i quali disporre la visita fiscale. Il Garante ha ritenuto il trattamento effettuato dall'Inps non conforme alla disciplina in materia di protezione dei dati personali, sanzionando l'Istituto con l'ordinanza ingiunzione 29 novembre 2018, n. 492 (doc. web n. 9078812).

L'Inps, infatti, pur avendo tempestivamente informato di aver sospeso l'utilizzo del predetto *software*, ha trattato, dall'8 febbraio 2011 al mese di marzo 2018, i dati personali relativi a 12,6 milioni di lavoratori privati assenti per malattia attraverso l'utilizzo del *software* "*Data Mining*/Savio" che attribuiva uno "*score* di probabilità" al certificato medico riferito al lavoratore, effettuando così un trattamento automatizzato di dati personali, anche idonei a rivelare lo stato di salute, raffrontando le informazioni contenute nel predetto certificato con le altre contenute nell'archivio gestionale delle visite mediche di controllo ed in ulteriori archivi amministrativi dell'Istituto.

Il trattamento, che non era stato sottoposto a verifica preliminare ai sensi dell'art. 17, d.lgs. n. 196/2003 né notificato al Garante, era stato effettuato in base a norme che, nonostante riconoscano l'obbligo di disporre delle visite domiciliari di controllo dei lavoratori assenti dal servizio per malattia e introducano la trasmissione telematica delle certificazioni di malattia sia per il settore pubblico che privato, non dispongono nulla in merito ai tipi di dati e alle operazioni eseguibili nell'ambito del trattamento automatizzato in argomento, in violazione quindi di quanto statuito dagli artt. 14 e 20, d.lgs. n. 196/2003. Inoltre, con specifico riferimento ai dati sensibili, il trattamento è stato effettuato senza che venisse resa agli interessati la prescritta informativa.

Controlli sulle prestazioni previdenziali e assistenziali

Il Garante si è espresso favorevolmente sulla modifica del regolamento per il trattamento dei dati sensibili e giudiziari dell'Inps, volta ad integrare, in particolare, l'all. n. 1, denominato "Prestazioni pensionistiche di natura previdenziale ed assistenziale - Gestione conto assicurato/pensionato". L'aggiornamento del predetto regolamento ha consentito all'Istituto di semplificare, nel rispetto del Codice, i controlli sulle prestazioni previdenziali e assistenziali, acquisendo in via telematica i dati e le informazioni personali che altre amministrazioni detengono per obblighi istituzionali, al fine di ridurre gli adempimenti dei cittadini e rafforzare il contrasto alle evasioni e alle frodi fiscali e contributive, nonché accertare il diritto e la misura delle prestazioni previdenziali, assistenziali e di sostegno al reddito. Sulla base di tale modifica normativa, l'Istituto ha quindi previsto di stipulare una convenzione con il Ministero della salute al fine acquisire, nel rispetto del principio di indispensabilità con le misure di sicurezza adeguate, attraverso le Schede di dimissione ospedaliera (flusso Sdo), i soli dati necessari a rilevare eventuali periodi di ricovero conti-

nuativo di durata superiore a 29 giorni, nell'anno solare di riferimento, riferibili ai titolari di indennità di accompagnamento, di indennità di frequenza e di assegno sociale e di assegno sociale sostitutivo di invalidità civile al fine di verificare la misura di tali prestazioni che deve essere ridotta in caso di ricoveri con rette a carico di enti pubblici. Tali verifiche vengono svolte nei confronti di coloro che non presentano all'Inps la prevista dichiarazione di responsabilità, nonché nei confronti di un campione di soggetti che presentano la richiesta dichiarazione o certificazione, ai fini del controllo di veridicità delle stesse, per l'eventuale attivazione dei recuperi di cui all'art. 1, commi 252 e 253, l. 23 dicembre 1996, n. 662.

Monitoraggio dei livelli essenziali delle prestazioni sociali

Il Garante ha espresso parere favorevole sullo schema di Accordo tra il Ministro del lavoro e delle politiche sociali, le regioni e Province autonome di Trento e Bolzano e le autonomie locali per l'avvio della sperimentazione in materia di banca dati delle valutazioni e progettazioni personalizzate, di cui al decreto legislativo 15 settembre 2017, n. 147.

In particolare, nelle more della realizzazione del Sistema informativo unitario dei servizi sociali (Siuss), per le finalità di ricognizione dei bisogni sociali, dei servizi sociali e di tutte le altre informazioni necessarie alla programmazione, alla gestione, al monitoraggio e alla valutazione delle politiche sociali, il Ministero del lavoro e delle politiche sociali ha voluto dare avvio alla sperimentazione dei flussi relativi alla banca dati delle valutazioni multidimensionali (componente del Casellario dell'assistenza istituito presso l'Inps relativa alle prestazioni sociali associate a una presa in carico da parte del servizio sociale, cd. flussi Sina e Sinba), sulla base della disciplina vigente, adottata in conformità alle indicazioni del Garante. Ciò, con particolare riferimento ai flussi necessari a monitorare l'utilizzo del Fondo per le non autosufficienze e del Fondo per l'assistenza alle persone con disabilità grave prive di sostegno familiare (Fondo cd. dopo di noi), finalizzati alla definizione di specifici livelli essenziali delle prestazioni e alla messa a punto del Piano per la non autosufficienza. Considerato che l'Accordo esaminato dal Garante ha previsto l'istituzione di una "Cabina di regia", composta da rappresentanti dell'Inps, dell'Anci e delle regioni e Province autonome, per il predetto monitoraggio, l'Autorità ha richiesto al Ministero del lavoro e delle politiche sociali di comunicare gli aspetti rilevanti in materia di protezione dei dati personali all'esito della predetta sperimentazione (parere 22 febbraio 2018, n. 101, doc. web n. 8145482).

5 La sanità e i dati genetici

5.1. *I trattamenti per fini di cura*

Diverse sono state le pronunce dell'Autorità con riferimento al trattamento dei dati per fini di cura. Merita particolare attenzione un provvedimento adottato nei confronti di una fondazione, che si occupa di assistenza geriatrica, la quale aveva sottoposto a verifica preliminare, ai sensi dell'art. 17, d.lgs. n. 196/2003, un trattamento di dati da effettuare attraverso un articolato sistema di monitoraggio, anche a distanza, di pazienti non auto-sufficienti, basato sull'uso di un bracciale o una cavigliera dotati di un localizzatore e di un misuratore di frequenza cardiaca. In particolare, il dispositivo avrebbe consentito la localizzazione del paziente soltanto all'interno dell'articolata struttura di cura e al verificarsi di determinati eventi suscettibili di esporre al pericolo il paziente; ciò avrebbe altresì determinato l'attivazione di una "telecamera di zona", con conseguente registrazione delle immagini per circa trenta minuti e invio di un messaggio di allerta al personale, al fine di renderne possibile il tempestivo intervento. Il Garante, considerate le finalità di prevenzione, diagnosi e cura perseguite attraverso tale sistema e l'estrema delicatezza dei dati trattati, aveva ritenuto opportuno prescrivere ulteriori misure, oltre a quelle già previste dalla fondazione (tra le quali l'acquisizione di un consenso specifico e ulteriore rispetto a quello già fornito dall'interessato all'atto di ingresso in struttura), al fine di innalzare il livello di tutela e assicurare la dignità dei pazienti. In particolare, è stato prescritto che il bracciale o la cavigliera avrebbero dovuto essere applicati con le modalità meno invasive per il paziente, al quale, qualora le condizioni lo avessero consentito, avrebbe dovuto essere fornita un'informativa sul trattamento dei dati personali adeguata alle sue capacità di comprensione. Inoltre, il giudizio della commissione interna alla struttura istituita per stabilire la necessità di una sorveglianza continua attraverso un dispositivo indossabile, avrebbe dovuto essere oggetto di valutazione periodica, così come, almeno ogni settimana, avrebbe dovuto essere verificata la regolarità del funzionamento e la corretta attribuzione del bracciale o della cavigliera al singolo paziente, al fine di evitare il verificarsi di scambi o altri comportamenti che avrebbero potuto alterarne la funzionalità (provv. 25 gennaio 2018, n. 29, doc. web n. 7810766).

Con riferimento ai malati di Alzheimer, è stato formulato un quesito in ordine all'installazione di un sistema di videosorveglianza presso un reparto di una casa di riposo ove gli stessi sono ospitati. In particolare, è stato evidenziato, con specifico riferimento alla possibilità di posizionare alcuni *monitor* in corridoio e nella sala da pranzo/soggiorno della struttura, la necessità di adottare specifici accorgimenti per salvaguardare la dignità degli interessati ed evitare la diffusione dei dati personali relativi alla salute, espressamente vietata dall'art. 2-*septies*, comma 8, del Codice. È stato rappresentato (cfr. nota 19 novembre 2018), in ogni caso, che il titolare, prima di procedere al trattamento, è tenuto ad effettuare una valutazione d'impatto sulla protezione dei dati personali oggetto di trattamento che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità del trattamento (art. 35 del RGPD e considerando 75; cfr., altresì, punto III.B. 7 delle Linee guida concernenti la valutazione di impatto sulla

protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del RGPD adottate dal Gruppo Art. 29 (WP248) il 4 aprile 2017 e successivamente emendate e adottate il 4 ottobre 2017, nel quale è espressamente indicato, tra i citati criteri, il trattamento dei dati relativi a interessati vulnerabili, quali anziani e pazienti) (cfr. successivo par. 5.4.2).

5.1.1. L'informativa e il consenso al trattamento dei dati sanitari

Specifiche istanze sono pervenute anche in relazione alla comunicazione di dati personali sulla salute. Tra queste una richiesta della Direzione di programmazione economica e di bilancio di una regione volta ad acquisire copia del verbale Inps "senza gli *omissis*" per permettere l'istruttoria della pratica di esenzione bollo auto in caso di invalidità grave; a questo proposito l'Ufficio, oltre a ricordare il principio secondo il quale i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (cd. principio di "minimizzazione dei dati"; art. 5, par. 1, lett. *c*), del RGPD), ha richiamato il provv. 16 febbraio 2011, n. 69 (doc. web n. 1792975), secondo il quale, considerato che "le certificazioni mediche che devono corredare le richieste relative alle diverse disabilità ammesse ai benefici fiscali" sono destinate a circolare tra i diversi soggetti (anche di natura privata) coinvolti (ciascuno per quanto di competenza) nelle procedure di valutazione dei requisiti legali di disabilità, deve essere garantita la rigorosa applicazione del principio di pertinenza sin dal momento della iniziale redazione della documentazione da parte degli operatori sanitari (tra i quali, ad es., le commissioni mediche previste dalla legge). La non indispensabilità dell'indicazione dei dati personali relativi alla diagnosi accertata in sede di visita medica risulta peraltro dal fatto "che la normativa di settore, se da un lato richiede la certificazione dello stato di «handicap grave» di cui all'art. 3, comma 3, l. n. 104/1992, in molti casi imponendo anche un'esplicita evidenziazione della gravità della patologia (ad es., con riguardo alla natura psichica o mentale della stessa), tuttavia non prevede come indispensabile l'indicazione della specifica patologia diagnosticata all'interessato" (cfr. punto 4.2, provv. 16 febbraio 2011, n. 69, cit.; provv. 21 marzo 2007, doc. web n. 1395821; v. anche provv.ti 21 aprile 2009, doc. web n. 1616870; 9 novembre 2005, doc. web n. 1191411) (nota 4 luglio 2018).

Sempre in materia di comunicazione di dati sulla salute, l'Ufficio ha risposto a un quesito di un medico in merito alla possibilità – alla luce dei chiarimenti contenuti nella lettera inviata dal Presidente del Garante alla Federazione italiana medici di medicina generale e al Consiglio nazionale dei presidenti degli Ordini dei medici chirurghi e degli odontoiatri (doc. web n. 3533561) – di mettere a disposizione, su richiesta del paziente, le sue ricette appendendole su una bacheca esterna allo studio medico, posta all'interno dell'edificio, con una indicazione esterna del nome del paziente. Al richiedente, è stato fatto osservare che tali modalità di consegna delle prescrizioni mediche non sono in linea con le indicazioni evidenziate dal Garante sul punto, secondo le quali "le procedure, in vigore già da tempo, consentono ai medici di lasciare ai pazienti ricette e i certificati presso le sale d'attesa dei propri studi o presso le farmacie, senza doverglieli necessariamente consegnare di persona. Per impedire la conoscibilità da parte di estranei di dati delicati, come quelli sanitari, è però indispensabile che ricette e certificati vengano consegnati in busta chiusa. La busta chiusa è tanto più necessaria nel caso in cui non sia il paziente a ritirare i documenti, ma una persona da questi appositamente delegata" (cfr. comunicato stampa 14 novembre 2015, doc. web n. 3533579) (nota 21 marzo 2018).

Con riferimento alla comunicazione di dati personali, anche non relativi alla salute, è stato fornito riscontro a un quesito in merito alla possibilità di consentire a terzi la visualizzazione dei dati di dettaglio sulla formazione continua per la verifica della regolarità formativa del professionista. In particolare, nel richiamare la specifica disciplina di settore che prevede l'obbligo per il professionista di seguire percorsi di formazione continua (aggiornamento professionale e formazione permanente), la cui violazione determina un illecito disciplinare (artt. 16-*bis* e 16-*ter*, d.lgs. 30 dicembre 1992, n. 502 e art. 3, comma 5, lett. *b*), d.l. 13 agosto 2011, n. 138, convertito con modificazioni in legge 14 settembre 2011, n. 148), è stato rappresentato che, secondo lo statuto del Consorzio gestione anagrafica delle professioni sanitarie (Co.Ge.A.P.S.), è espressamente vietato al Consorzio acquisire, vantare o cedere a terzi diritti di proprietà o di uso autonomo di tali dati al di fuori del perseguimento degli scopi consortili, che concernono esclusivamente la gestione dell'Anagrafe nazionale dei crediti formativi Ecm, nonché attività di studio e reperimento di fondi ed infrastrutture utili allo scopo della formazione continua (art. 2). Pertanto, alla luce del quadro normativo sopra richiamato, non risulta, allo stato, possibile per il Consorzio consentire a terzi la visualizzazione del numero di crediti formativi conseguiti da ogni singolo professionista (nota 24 aprile 2018).

5.1.2. Il Fascicolo sanitario elettronico (Fse) e il dossier *sanitario*

Con riferimento a trattamenti di dati personali effettuati attraverso il Fse il Garante ha fornito un parere in merito a uno schema di decreto volto a potenziare i servizi telematici resi disponibili dall'Infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario – Fse (Ini) di cui al decreto del Mef 4 agosto 2017 e a evitare disservizi per l'assistito in caso di un suo trasferimento per l'assistenza verso una regione o provincia autonoma in cui non sia ancora operativo il Fse. Le osservazioni formulate dall'Ufficio hanno inteso assicurare, da una parte, la delimitazione dei nuovi servizi resi disponibili dall'Ini e la garanzia di un accesso *online* al Fse precedentemente istituito dall'altra, richiamare il Mef alla tenuta, attraverso l'Ini, dell'indice dei documenti sanitari e di quello relativo ai metadati dei documenti sanitari, relativi agli assistiti, risultanti nell'anagrafe nazionale degli assistiti, individuando le necessarie misure per assicurare il rispetto del principio di limitazione della conservazione (parere 27 settembre 2018, n. 456, doc. web n. 9054337).

L'Ufficio continua a dialogare con le istituzioni coinvolte nella realizzazione del Fse (Ministero della salute, Mef, regioni) in merito all'applicazione della disciplina in materia di protezione dei dati personali ai trattamenti effettuati attraverso il fascicolo anche alla luce dei nuovi adempimenti dettati dal RGPD.

Numerose sono state le istruttorie avviate in merito ai trattamenti di dati personali effettuati attraverso i Fse regionali. In particolare, in un caso è stato accertato l'erroneo inserimento nei documenti disponibili nel Fascicolo di alcune lettere di dimissione ospedaliera riferite ad altri pazienti. A seguito dell'intervento dell'Ufficio è stato modificato il flusso di integrazione dei documenti, prevedendo la consistenza dei messaggi per mezzo di intervalli temporali predefiniti, finalizzati ad evitare errori di concorrenza che hanno determinato l'incongruenza dei dati. In considerazione dell'illecita comunicazione a terzi di dati personali di natura sensibile presenti nelle lettere di dimissione ospedaliera di terzi da parte del titolare, è stato avviato un procedimento sanzionatorio (nota 17 gennaio 2018).

***Dossier* sanitario**

In merito ai trattamenti effettuati attraverso il *dossier* sanitario sono proseguite le istruttorie nei confronti delle strutture sanitarie, sia pubbliche che private, dalle quali è emersa una crescente conformità alle indicazioni fornite dall'Autorità nelle

Linee guida in materia di *dossier* sanitario (provv. 4 giugno 2015, n. 331, doc. web n. 4084632).

Permangono, tuttavia, sistemi informativi riconducibili al *dossier* sanitario ancora non pienamente conformi al dettato normativo. Al riguardo, in occasione di un'attività ispettiva presso una struttura ospedaliera, è stata riscontrata la mancanza degli specifici adempimenti previsti dalla disciplina in materia di protezione dei dati personali con riferimento ai trattamenti effettuati nell'ambito del *dossier* sanitario aziendale. A seguito dell'intervento dell'Ufficio, l'ospedale ha posto in essere una pluralità di azioni correttive che hanno riguardato la manifestazione del consenso, le informazioni da rendere ai pazienti e la formazione del personale medico ed infermieristico (nota 15 ottobre 2018).

5.1.3. La tutela della dignità della persona

L'Autorità ha continuato a mostrare grande attenzione in merito al rispetto delle disposizioni del decreto legislativo n. 196/2003 e delle norme di settore volte ad assicurare la tutela della dignità delle persone nell'ambito dei trattamenti di dati personali per finalità di cura.

In un caso, l'Ufficio è intervenuto nei confronti di un operatore di un ospedale veneto il quale, in presenza di terzi, aveva richiesto alla segnalante presente in sala di attesa, dopo essere stata chiamata per cognome, se dovesse effettuare una interruzione di gravidanza. In particolare, è stato rivolto un richiamo al rispetto della dignità di pazienti sottoposti a trattamenti medici invasivi, nei cui confronti va prestata una particolare attenzione anche per effetto di peculiari obblighi di legge o di regolamento (ad es., in riferimento a individui sieropositivi o affetti da infezione da Hiv, a persone offese da atti di violenza sessuale o in casi di interruzione di gravidanza: cfr. punto 3.a), provv. 9 novembre 2005, doc. web n. 1191411). Nel caso di specie, l'ospedale ha quindi ribadito, nelle indicazioni dirette al personale sulla procedura da seguire, la necessità di evitare di chiamare l'utenza con il nome o di citare la prestazione alla quale la stessa si deve sottoporre manifestando l'intenzione di intervenire sul piano disciplinare in caso di accertata violazione da parte dei propri dipendenti (nota 19 luglio 2018).

Le medesime problematiche sono state evidenziate anche dopo l'entrata in vigore del RGPD; in particolare, è stata avviata un'istruttoria nei confronti di un ospedale nel quale un medico (in servizio presso lo stesso) non avrebbe rispettato, in occasione di una visita oculistica, le garanzie previste dalla legge a tutela della dignità e della riservatezza delle persone interessate, divulgando alcune informazioni del loro stato di salute, ivi compresa la presunta causa della malattia, a terzi. In particolare, è stato ritenuto compatibile con il RGPD e con le disposizioni del decreto legislativo n. 101/2018*,* l'art. 83 del Codice (cfr. art. 22, comma 11, d.lgs. n. 101/2018 e il punto 3.*b*) del citato provv. 9 novembre 2005; art. 22, comma 4, d.lgs. n. 101/2018). Pertanto, è necessario che siano adottate idonee cautele in relazione allo svolgimento di colloqui, specie con il personale sanitario (ad es. in occasione di prescrizioni o di certificazioni mediche), per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità in concreto utilizzate (nota 9 novembre 2018).

5.1.4. Il trattamento di dati personali in relazione all'accertamento dell'infezione da Hiv

Con specifico riferimento alle misure a tutela della dignità e della riservatezza dei malati di Hiv in occasione dell'erogazione di prestazioni sanitarie, l'Ufficio è inter-

venuto fornendo specifiche indicazioni in merito alla possibilità da parte degli esercenti le professioni sanitarie di comunicare lo stato di sieropositività di una paziente, alle persone più vicine alla stessa, con particolare riguardo al *partner*, anche in assenza di consenso dell'interessata; ciò in quanto la stessa paziente si era rifiutata di comunicare al *partner* la propria condizione esponendolo al rischio di contagio.

La questione prospettata è apparsa meritevole di considerazione, attesa l'estrema delicatezza degli interessi coinvolti, ed è stata affrontata sottolineando da un canto che il decreto legislativo n. 196/2003 prevedeva in capo agli organismi sanitari e agli esercenti le professioni sanitarie l'obbligo di operare con il consenso dell'interessato, potendone tuttavia prescindere, sulla base dell'autorizzazione del Garante, qualora si fosse dovuto tutelare la salute o l'incolumità fisica di un terzo e l'interessato si fosse rifiutato o fosse impossibilitato a prestare il consenso (v. autorizzazione generale n. 2 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale); dall'altro, evidenziando che il richiamato decreto legislativo non conteneva deroghe alle disposizioni di legge che stabiliscono "divieti o limiti più restrittivi" in materia di trattamento di taluni dati personali. Tale deve considerarsi anche la legge 5 giugno 1990, n. 135, in tema di Aids e Hiv, nella quale figura, in particolare, l'obbligo di comunicare i risultati di accertamenti diagnostici diretti o indiretti per l'infezione da Hiv alla sola persona cui tali esami si riferiscono (art. 5, comma 4). Pertanto, è stato ritenuto che, ai fini della comunicazione ai familiari dello stato di sieropositività del paziente, vada ricercato il consenso della persona interessata in tutti i modi possibili. In proposito, è stata valutata l'opportunità che il medico provvedesse a sensibilizzare la persona sieropositiva circa il grave rischio per la vita del *partner* ingenerato da un suo comportamento omissivo, cercando di persuaderla a comunicare a questi la propria sieropositività oppure a manifestare il proprio consenso alla rivelazione da parte dello stesso medico (cfr. al riguardo le Linee guida dell'Organizzazione Mondiale della Sanità del dicembre 2016 sul test di autodiagnosi Hiv e la notifica volontaria al *partner*, reperibili in http://www.who.int/hiv/pub/vct/hiv-self-testing-guidelines/en/; la Raccomandazione del Consiglio d'Europa No. R (89) 14 nel settore della sanità e nel contesto sociale, reperibile in https://rm.coe.int/09000016804caf46; le *faq* del Ministero della salute su Hiv e Aids). Ciò anche alla luce delle possibili responsabilità penali del soggetto che, consapevole del proprio stato patologico, ometta di informare il *partner* (cfr. artt. 582-583 c.p., nonché Cass. pen. n. 30425/2001). Sempre sotto il profilo penale, possono essere tenute parimenti in considerazione le riflessioni in ambito giuridico e scientifico circa i presupposti per l'eventuale applicazione dell'esimente dello stato di necessità (art. 54 c.p.) o della "giusta causa" – richiamata anche dalle norme di deontologia medica – che legittimerebbe la rivelazione di informazioni eventualmente coperte da segreto professionale (art. 622 c.p., nonché codice di deontologia medica 2014, artt. 10, 12 e 34) nel caso in cui la sieropositività sia resa nota dal medico senza il consenso dell'interessato a un suo familiare, allorché vi sia l'urgenza di salvaguardare l'integrità psico-fisica del familiare medesimo, laddove sia in grave (e altrimenti non evitabile) pericolo la salute o la vita di questi (nota 9 marzo 2018).

Il richiamo alla specifica normativa in ordine alla comunicazione di risultati di accertamenti diagnostici per l'infezione da Hiv è stato altresì rivolto a un Servizio di politiche del lavoro e formazione professionale provinciale, il quale, nell'ambito della richiesta della visita sanitaria di controllo, aveva trasmesso copia della documentazione sanitaria dalla quale si evinceva la diagnosi di Hiv anche alla società presso la quale l'interessato prestava la propria attività lavorativa. In tale occasione, nel rilevare la sussistenza di specifici obblighi normativi nei riguardi del lavoratore

per consentire al datore di lavoro di verificare le sue reali condizioni di salute nelle forme di legge, è stato evidenziato che, per attuare tali obblighi è, ad esempio, previsto che venga fornita all'amministrazione di appartenenza un'apposita documentazione a giustificazione dell'assenza, consistente in un certificato medico contenente la sola indicazione dell'inizio e della durata presunta dell'infermità (cd. prognosi). È stato inoltre precisato che, in assenza di speciali disposizioni di natura normativa che dispongano diversamente per specifiche figure professionali, il datore di lavoro pubblico non è mai legittimato a raccogliere certificazioni mediche contenenti anche l'indicazione della diagnosi (cfr. Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, 14 giugno 2007, doc. web n. 1417809). Pertanto, la predetta comunicazione di dati sulla salute non è risultata conforme alla disciplina in materia di protezione dei dati personali e in merito ad essa è stato avviato un procedimento sanzionatorio in ragione della illegittima comunicazione.

5.2. *I trattamenti di dati relativi alle condizioni di salute per fini amministrativi*

Dat

L'Autorità si è occupata degli aspetti relativi alla protezione dei dati personali delle disposizioni anticipate di testamento (Dat) previste dalla legge n. 219/2017. In particolare, l'Ufficio ha partecipato al tavolo di lavoro presso il Ministero della salute per la costituzione della banca dati nazionale delle Dat da istituire presso il Dicastero ai sensi della legge n. 205/2017.

In occasione dei lavori del tavolo è stata formulata una richiesta di parere al Consiglio di Stato, attesa la difficoltà interpretativa della normativa di settore e il necessario raccordo della stessa con le contestuali disposizioni in materia dettate dalla legge n. 205/2017. La richiesta di parere ha riguardato anche questioni legate all'effettiva utilizzabilità della banca dati nazionale Dat concernenti profili rilevanti rispetto al trattamento dei dati personali indicati nelle Dat. Il Consiglio di Stato, con parere del 18 luglio 2018, nel riconoscere le difficoltà interpretative delle norme che regolano la materia e la necessità di dare effettiva attuazione ai precetti legislativi, ha fornito indicazioni puntuali anche in merito al tenore letterale delle disposizioni contenute nelle predette normative. In particolare, è stato ritenuto che, su richiesta dell'interessato, copia delle Dat possa essere inviata alla banca dati nazionale da parte dell'Ufficiale di stato civile o della struttura sanitaria alle quali sono state consegnate. Il Consiglio di Stato ha inoltre precisato che alla banca dati nazionale potrà accedere il medico che ha in cura l'interessato e il fiduciario sino a quando è in carica.

Contestualmente ai lavori del tavolo per la costituzione della banca dati nazionale delle Dat, l'Ufficio è stato chiamato dalle regioni a interloquire in merito alla possibilità, conferita alle stesse dal legislatore nazionale, di regolamentare, entro limiti definiti, la raccolta di copia delle Dat in una banca dati regionale.

Al riguardo, nelle more della costituzione della banca dati nazionale, l'Ufficio ha richiamato gli interlocutori istituzionali a porre in essere sistemi "dialoganti", che assicurino livelli di protezione dei dati personali omogenei sul territorio nazionale, in un contesto in cui il principio di autodeterminazione informativa si affianca a quello dell'autodeterminazione terapeutica.

Inmp

Con riferimento al trattamento dei dati personali effettuato per finalità amministrative correlate alla cura da parte di organi centrali, si evidenzia il parere favorevole espresso dall'Autorità sullo schema di regolamento per il trattamento dei dati sensibili e giudiziari da parte dell'Istituto nazionale per la promozione della salute delle

5

popolazioni migranti e per il contrasto delle malattie della povertà (Inmp) ai sensi del previgente art. 20, d.lgs. n. 196/2003. Prima di rilasciare il predetto parere, in occasione di riunioni e contatti informali sono state formulate diverse osservazioni concernenti, in particolare: la corretta individuazione delle finalità di rilevante interesse pubblico per il cui perseguimento era necessario trattare dati sensibili e giudiziari; il richiamo al rispetto delle prescrizioni contenute in alcuni provvedimenti del Garante (v., ad es., provv.ti 12 novembre 2014, n. 515, doc. web n. 3624070; 21 aprile 2011, n. 160, doc. web n. 1809039); l'individuazione dell'ambito di comunicazione dei dati oggetto di trattamento e la previsione di opportune cautele a tutela della riservatezza degli interessati; la precisazione relativa agli ambiti di ricerca, con relativa indicazione dei presupposti normativi (provv. 15 febbraio 2018, n. 80, doc. web n. 8126123).

"Medicina di iniziativa"

A seguito di una comunicazione di violazione di dati personali, cui è seguito un accertamento ispettivo, l'Ufficio si è occupato del trattamento dei dati personali effettuato attraverso un sistema informativo regionale di reportistica e visualizzazione a disposizione dei medici di assistenza primaria (Medico di medicina generale e Pediatra di libera scelta - Mmg/Pls) i quali, tramite una *web application*, erano abilitati ad accedere ad un portale sulla continuità delle cure per l'utilizzo di diversi servizi di prevenzione e per l'invio alla regione dei dati personali oggetto di specifici obblighi normativi.

Il tema oggetto del predetto accertamento ispettivo richiama la tematica relativa alla possibilità per il Mmg/Pls di accedere ai documenti sanitari dell'assistito nell'ambito della cd. "medicina di iniziativa", ovvero un modello assistenziale orientato alla promozione attiva della salute dell'individuo, specie se affetto da malattie croniche o disabilità e alla responsabilizzazione delle persone nel proprio percorso di cura. Sul punto l'Ufficio in passato aveva già invitato il Ministero della salute a disciplinare quanto prima con un atto normativo un'attività così delicata, che presenta anche significativi risvolti etici (diritto di non sapere). È stato infatti evidenziato che non esiste nel nostro ordinamento giuridico una definizione e una disciplina specifica della cd. "medicina d'iniziativa" ancorché tale locuzione ricorra in numerosi atti di indirizzo e programmazione del Ministero della salute e delle regioni.

Nel corso dei predetti accertamenti è stato constatato che, con specifico riferimento ad alcune patologie croniche o a determinate malattie oncologiche, erano stati sviluppati, a livello regionale, strumenti di reportistica che, elaborando le informazioni oggetto dei flussi informativi verso la Regione mediante un algoritmo di calcolo che si basa su parametri statistici, mettono a disposizione dei Mmg/Pls un profilo sanitario di rischio dell'assistito, invitando il medico a proporre allo stesso specifici accertamenti diagnostici in chiave di prevenzione. Al riguardo, l'Ufficio ha evidenziato che l'adozione di tali sistemi determina la raccolta e l'elaborazione di dati sanitari al fine di realizzare, con riferimento a specifiche patologie, un profilo sanitario di rischio dell'interessato e configura quindi un trattamento autonomo e ulteriore rispetto a quello principale finalizzato alla cura dell'assistito (cfr. parere sullo schema di d.P.C.M. in materia di Fse, del 22 maggio 2014, doc. web n. 3230826, in merito alla realizzazione di "servizi di elaborazione di dati" per finalità di governo e di ricerca da parte delle regioni).

Ciò stante, l'Ufficio ha invitato la regione interessata, nel rispetto del principio di responsabilizzazione di cui al RGPD, a impostare l'attività sopra descritta nel rispetto dei presupposti di liceità (tra i quali il consenso informato dell'assistito), posto che lo stesso non risulta quale trattamento strettamente necessario per il perseguimento delle finalità di diagnosi e assistenza sanitaria perseguite dal Mmg/Pls. Agli enti coinvolti è stato ricordato che il titolare è tenuto ad effettuare una previa

valutazione dell'impatto dei trattamenti previsti sul diritto alla protezione dei dati personali, quando gli stessi possono presentare rischi elevati per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità del trattamento. Ove all'esito di tale valutazione risulti che i trattamenti presentino rischi elevati per i diritti e le libertà fondamentali degli interessati, in assenza di misure adottate dal titolare per attenuarli, il titolare è tenuto a consultare il Garante, prima di procedere al trattamento (artt. 35 e 36 del RGPD). Con specifico riferimento alla fattispecie oggetto di intervento, alla luce della natura dei dati trattati e della numerosità degli interessati, il trattamento in oggetto è stato considerato rientrante nei casi in cui il titolare non può prescindere da una valutazione di impatto sulla protezione dei dati, ai sensi di quanto previsto dal RGPD e dei criteri individuati dal Gruppo Art. 29 nelle Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del RGPD (WP 248 rev. 01 adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017).

Con riferimento, invece, all'aspetto che aveva determinato la comunicazione di violazione dei dati personali, a seguito dell'intervento dell'Ufficio, sono state adottate specifiche procedure per gestire gli eventi di *data breach*, consistenti nella rilevazione dell'evento di sicurezza, mitigazione, risoluzione, ripristino, analisi degli elementi per il miglioramento e reportistica. Al riguardo, la regione è stata sollecitata a verificare la corretta applicazione di quanto previsto dalle predette procedure, ad assicurarsi dell'effettiva de-indicizzazione dei contenuti riferibili a dati personali di assistiti e a prestare particolare attenzione, in occasione del rilascio di nuove funzionalità/migrazioni/aggiornamenti *software* e/o altri cambiamenti, al mantenimento delle corrette configurazioni dei permessi di accesso alle risorse (fisiche, logiche, etc.), in particolare, laddove siano presenti dati personali e dati relativi alla salute degli interessati (nota 9 luglio 2018).

Tra i casi sottoposti all'Ufficio relativi al trattamento dei dati personali connesso alle procedure amministrative, si evidenzia anche l'intervento nei confronti di un'azienda sanitaria affinché la stessa, su richiesta dell'interessato, fornisse una certificazione attestante l'invalidità civile di un minore, priva dell'indicazione degli estremi della sentenza del Tribunale dei minori di affidamento idonea a far desumere lo stato di adozione dello stesso. Sul punto l'azienda è stata, infatti, richiamata al rispetto delle specifiche garanzie di riservatezza previste dalla disciplina in materia di adozioni (cfr. art. 28, comma 3, legge n. 184/1983), relative al divieto per qualsiasi ente pubblico o privato, autorità o pubblico ufficio "di fornire notizie, informazioni, certificazioni, estratti o copie dai quali possa comunque risultare il rapporto di adozione" (nota 12 giugno 2018).

5.2.1. Il trattamento di dati personali nell'ambito dell'assolvimento degli obblighi vaccinali

È proseguita l'attività del Garante in ordine alla valutazione degli aspetti di protezione dei dati personali, connessi agli obblighi vaccinali previsti dall'art. 1, d.l. n. 73/2017, che, al fine di assicurare la tutela della salute pubblica e il mantenimento di adeguate condizioni di sicurezza epidemiologia in termini di profilassi e di copertura vaccinale, prevede per i minori di età compresa tra zero e sedici anni e per tutti i minori stranieri non accompagnati una serie di vaccinazioni obbligatorie e gratuite, in base alle specifiche indicazioni del Calendario vaccinale nazionale relativo a ciascuna coorte di nascita.

Come già anticipato nella Relazione 2017, con decreto legge 16 ottobre 2017, n. 14 (art. 18-*ter*), è stato previsto che, anche per l'anno scolastico 2017/2018, nelle

sole regioni e province autonome presso le quali sono già state istituite anagrafi vaccinali, le disposizioni di semplificazione già previste per l'a.s. 2019/2020 – relative alla possibilità che le aziende sanitarie locali restituiscano alle scuole gli elenchi dei soggetti che risultano non in regola con gli obblighi vaccinali – siano applicabili a decorrere dall'anno scolastico 2018/2019, nel rispetto delle modalità operative congiuntamente definite dal Ministero della salute e dal Miur, sentito il Garante. Il predetto decreto prevede poi che nelle medesime regioni e province autonome, le disposizioni di semplificazione sopra richiamate siano applicabili già per l'anno scolastico in corso, a condizione che il controllo sul rispetto degli adempimenti vaccinali si fosse concluso entro il 10 marzo 2018.

Al riguardo, il Garante è stato chiamato ad esprimere il proprio parere in merito ad un documento recante "Modalità tecniche per lo scambio dei dati relativi alla situazione vaccinale degli iscritti tra le istituzioni scolastiche/educative e formative e l'Azienda sanitaria locale competente", da allegarsi alla circolare allo scopo predisposta dai competenti uffici del Ministero della salute e del Miur.

Il predetto documento prevedeva due modalità di scambio dei dati: tramite lo strumento della Pec e tramite un sistema informativo *web based*, messo a disposizione dalla Regione o dalla Provincia autonoma, a cui i dirigenti delle istituzioni del sistema nazionale di istruzione e i responsabili dei servizi educativi per l'infanzia, dei centri di formazione professionale regionale e delle scuole private non paritarie potevano accedere tramite adeguate credenziali.

Il parere è stato reso su una versione che ha tenuto conto degli approfondimenti e di alcune osservazioni formulate dall'Ufficio, all'esito di riunioni e contatti informali, che hanno riguardato, ad esempio, gli aspetti relativi alla necessità di conformare al dettato normativo (art. 3-*bis*, comma 2, d.l. n. 73/2017) le diciture che le aziende sanitarie competenti devono completare quando restituiscono gli elenchi degli iscritti ricevuti dagli istituti scolastici; la necessità di circoscrivere le informazioni da scambiare per consentire l'identificazione certa di ogni iscritto (ritendendosi eccedente l'indicazione dell'indirizzo di residenza e di domicilio); la possibilità di valutare l'istituzione di una Pec dedicata.

Nello stesso parere è stato suggerito, con riferimento alla modalità di invio dei dati tramite funzionalità *web*, di effettuare un sistema "*single sign on-SSO*" tra i sistemi regionali e il sistema informativo dell'istruzione (Sidi) del Miur, al fine di semplificare le procedure di autenticazione ai portali regionali da parte dei dirigenti scolastici, evitando al contempo la proliferazione delle credenziali di autenticazione (provv. 22 febbraio 2018, n. 117, doc. web n. 7873593).

L'Autorità è stata ulteriormente interessata al fine di fornire il proprio parere nell'ambito della normativa attuativa del decreto legge n. 73/2017. In particolare, ha fornito un parere sullo schema di decreto ministeriale relativo all'istituzione e al funzionamento dell'anagrafe nazionale vaccini, da crearsi ai sensi dell'art. 4-*bis* del citato d.l. n. 73/2017 e contenente i dati dei soggetti vaccinati e da sottoporre a vaccinazione, nonché i soggetti di cui sia stata accertata l'avvenuta immunizzazione a seguito di malattia naturale e quelli nei cui confronti le vaccinazioni possono essere omesse o differite per accertato pericolo per la salute, in relazione a documentate condizioni cliniche, oltre alle informazioni relative alle dosi e ai tempi di somministrazione delle vaccinazioni effettuate e agli eventuali effetti indesiderati.

Secondo quanto previsto dalla disciplina di settore, l'anagrafe nazionale vaccini (Anv) raccoglie i dati delle anagrafi regionali vaccinali (Arv) esistenti, i dati relativi alle notifiche effettuate dal medico curante nell'ambito del Sistema informativo delle malattie infettive e diffusive nonché i dati concernenti gli eventuali effetti indesiderati delle vaccinazioni che confluiscono nella rete nazionale di farmacovigilanza.

Anche in questo caso, il parere è stato reso a seguito di contatti e riunioni informali con il Ministero della salute nell'ambito dei quali sono stati introdotti dei miglioramenti, aventi ad oggetto, tra gli altri, la corretta individuazione della titolarità del trattamento delle anagrafi regionali vaccinali e della tipologia dei dati ivi trattati in relazione alle finalità perseguite; il sistema di notifiche garantito dall'anagrafe nazionale vaccini, al fine di consentire l'aggiornamento delle anagrafi regionali; il periodo di conservazione dei dati personali raccolti nell'anagrafe nazionale; l'esclusione del raccordo dell'anagrafe nazionale vaccini con il Nuovo sistema informativo del Ministero della salute; le modalità di accesso ai dati dell'anagrafe nazionale da parte del Ministero della salute e delle regioni e province autonome; le misure tecniche e organizzative per la gestione dei supporti di memorizzazione, per l'abilitazione ai servizi che prevedono l'accesso a dati riferiti ai singoli assistiti e per la registrazione nei file di *log*.

In ogni caso, è stato precisato che, in considerazione della piena applicazione del RGPD, nel fornire agli interessati le informazioni sul trattamento dei dati personali effettuato attraverso le predette anagrafi, devono essere fornite anche le informazioni supplementari previste dagli artt. 13 e 14 del richiamato Regolamento rispetto a quelle stabilite dal decreto legislativo n. 196/2003 (provv. 26 luglio 2018, n. 438, doc. web n. 9025504).

5.3. *La ricerca in ambito sanitario*

Per quanto riguarda il settore della ricerca, una clinica privata accreditata ha sottoposto all'attenzione del Garante la richiesta ricevuta da una azienda sanitaria volta ad ottenere l'acquisizione delle cartelle cliniche relative a pazienti affetti da patologia neoplastica, residenti nel territorio dell'azienda e soggetti al ricovero presso la stessa clinica, nell'ambito dell'attività correlata alla gestione del registro tumori della regione di appartenenza. La questione è stata ricondotta alla specifica disciplina di settore, concernente i sistemi di sorveglianza e i registri di patologia (art. 12, commi 11, 12 e 13, d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 221; d.P.C.M. 3 marzo 2017, con il parere del Garante reso in data 23 luglio 2015, n. 435, doc. web n. 4252386, nonché, nel caso considerato, sul registro tumori di popolazione della Regione Campania: legge regionale 10 luglio 2012, n. 18). Alla luce del richiamato quadro normativo, poiché nella predetta legge regionale n. 18/2012 non è stato possibile rinvenire le indicazioni richieste dall'art. 12, comma 13, d.l. n. 179/2012, è stato ritenuto che la comunicazione dei dati sanitari prevista non potesse avvenire in assenza di accorgimenti tecnici idonei a garantire un adeguato livello di sicurezza dei dati, quali quelli necessari per non rendere identificabili gli interessati e per minimizzare i rischi di re-identificazione degli stessi (nota 8 marzo 2018).

Al Garante è stato altresì richiesto di esprimere un parere circa alcuni schemi di regolamento aventi ad oggetto il funzionamento dei registri tumori. In particolare, la Provincia autonoma di Bolzano ha sottoposto all'Autorità uno schema di regolamento per disciplinare il citato registro (istituito dalla legge della Provincia autonoma di Bolzano n. 7 del 5 marzo 2001), che raccoglie dati relativi a persone affette da neoplasie a fini di studio e di ricerca scientifica in campo medico, biomedico ed epidemiologico.

In occasione di riunioni preliminari sono stati formulati alcuni rilievi in merito, in particolare, alla corretta designazione dell'Osservatorio epidemiologico provinciale quale responsabile del trattamento dei dati personali, all'esigenza di un

richiamo al principio di indispensabilità previsto per il trattamento dei dati sensibili e, infine, all'individuazione della periodicità con la quale il titolare del trattamento del Registro raccoglie i dati dall'archivio regionale delle schede di dimissioni ospedaliere della Provincia. Tali osservazioni sono state recepite dalla Provincia autonoma di Bolzano richiamata comunque, nell'ambito del parere reso, all'adeguamento di alcune disposizioni dello schema al RGPD (provv. 29 marzo 2018, n. 178, doc. web n. 8983322).

Anche la Conferenza delle Regioni e delle Province autonome di Trento e Bolzano, organismo di coordinamento e di indirizzo delle Regioni e delle Province autonome, ha sottoposto al Garante uno "Schema tipo di regolamento recante norme per il funzionamento del registro tumori della Regione/Provincia autonoma". Tale documento costituisce lo schema tipo in conformità al quale ciascuna Regione e Provincia autonoma potrà adottare il proprio regolamento, in modo tale che soltanto ove si intendano apportare modifiche sostanziali o integrazioni non formali riguardanti il trattamento dei dati personali rispetto allo schema tipo in esame, i predetti enti dovranno chiedere all'Autorità uno specifico parere su tali modifiche/integrazioni.

Il documento è stato elaborato anche a seguito di una lunga attività di collaborazione con il Garante che, durante incontri e interlocuzioni, ha formulato osservazioni, poi recepite dalla stessa Conferenza, riguardanti anzitutto la corretta individuazione delle finalità di rilevante interesse pubblico; il rispetto del principio di necessità nel trattamento dei dati previsto per le attività di gestione, controllo e valutazione dell'assistenza sanitaria; la selezione dei dati sensibili raccolti presso gli archivi delle strutture sanitarie regionali/provinciali per implementare e aggiornare il registro; le modalità per fornire l'informativa agli interessati; le cautele relative alla pseudonimizzazione dei dati destinati a confluire nel registro tumori e alla trasmissione di documenti cartacei; l'individuazione di congrui periodi di conservazione dei dati sensibili presenti nel registro e dei *file* di *log* relativi alle operazioni di accesso.

Anche in tale caso, nell'ambito del parere reso, è stata evidenziata l'esigenza di adeguare le pertinenti disposizioni dello schema tipo in vista dell'imminente applicazione del RGPD (provv. 18 aprile 2018, n. 227, doc. web n. 8983816).

5.4. *Prime attività derivanti dal RGPD e dal decreto legislativo n. 101/2018*

5.4.1. L'esercizio dei diritti

L'Ufficio ha altresì avuto modo di fornire i necessari chiarimenti sulle procedure da seguire in caso di esercizio dei diritti aventi ad oggetto dati sulla salute sulla base di quanto stabilito dal RGPD.

In particolare, a una istante che aveva formulato un ricorso prima dell'entrata in vigore del decreto legislativo n. 101/2018, è stato rappresentato che, considerata la necessità di conformare le norme del decreto legislativo n. 196/2003 al RGPD, l'Autorità, con delibera 31 maggio 2018, n. 374 (doc. web n. 8997237), aveva disposto la disapplicazione delle norme sulla procedura dei ricorsi contenute nella Sezione III del Capo I del titolo I del menzionato decreto in quanto ritenute incompatibili con le disposizioni relative ai reclami di cui agli artt. 77 ss. del RGPD.

Alla luce di quanto sopra, l'istanza proposta in veste di "ricorso" è stata esaminata a titolo di "reclamo" secondo la procedura già prevista dagli artt. 142 ss. del decreto legislativo n. 196/2003 in quanto compatibile con il nuovo quadro normativo (artt.

77 e ss. del RGPD). È stato altresì rappresentato che il RGPD (e anteriormente anche il decreto legislativo n. 196/2003) prevede il diritto dell'interessato di ottenere dal titolare del trattamento "l'accesso ai dati personali" e alle altre specifiche informazioni sul trattamento dei dati allo stesso riferiti (artt. 15 e ss.) e che la violazione delle richiamate disposizioni, qualora accertate, sono ora soggette a sanzione amministrativa pecuniaria (v. art. 83, par. 5, lett. *b*), del RGPD). Al titolare è stato quindi chiesto di aderire alle richieste dell'interessato e di informarlo circa le determinazioni adottate, inviando copia del riscontro anche all'Autorità (nota 31 luglio 2018).

Similmente, l'Autorità è intervenuta nei confronti di un'azienda ospedaliera, in relazione al parziale riscontro fornito all'istanza formulata dal reclamante, in quanto la cartella clinica della quale è stata fornita copia sarebbe risultata priva dell'esame diagnostico relativo ad una ecografia addominale effettuata dallo stesso reclamante durante la degenza. A seguito della richiesta dell'Ufficio, volta ad ottenere riscontro in ordine alla predetta istanza, la medesima azienda ha comunicato di aver aderito alla richiesta del reclamante (nota 12 novembre 2018).

5.4.2. La valutazione di impatto in ambito sanitario

In più di una occasione l'Autorità ha avuto modo di fornire delle indicazioni in ordine all'applicazione del RGPD, con particolare riferimento alla valutazione di impatto sulla protezione dei dati in ambito sanitario.

In particolare, un'associazione – che aveva comunicato l'intenzione di dotare gli automezzi adibiti al trasporto degli utenti diversamente abili di un sistema integrato di monitoraggio e videosorveglianza al fine di tutelare la salute e l'incolumità degli utenti quotidianamente accompagnati dall'abitazione ai presidi riabilitativi – è stata invitata a rispettare il principio di indispensabilità dei dati personali trattati. Ciò considerata la particolare delicatezza del trattamento ipotizzato, consistente anche in una timbratura del *badge* degli utenti per la registrazione della loro salita e discesa dal mezzo, unitamente a un sistema di localizzazione tramite Gps e a una raccolta di una serie di informazioni degli utenti (comprese le cartelle cliniche). Il titolare è stato quindi invitato a effettuare una valutazione d'impatto sulla protezione dei dati e a consultare il Garante prima di procedere al trattamento ove, all'esito della predetta valutazione, fosse risultato un rischio elevato del trattamento nonostante le misure adottate per attenuarlo (artt. 35 e 36 del RGPD).

La predetta valutazione di impatto avrebbe dovuto tener conto di alcuni provvedimenti, già adottati dall'Autorità, nelle materie alle quali la stessa si riferisce, da tenere in considerazione quale parametro di riferimento; tra questi il provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680), i provvedimenti in materia di localizzazione dei veicoli (cfr., *ex multis*, provv.ti 5 giugno 2008, doc. web n. 1531604; 4 ottobre 2011, n. 270, doc. web n. 1850581; 29 novembre 2012, n. 368, doc. web n. 2257616; 7 marzo 2013, n. 103, doc. web n. 2471134; 25 febbraio 2016, n. 78, doc. web n. 4807812) e, da ultimo, al provvedimento di verifica preliminare, relativo alla raccolta di dati attraverso il monitoraggio a distanza di pazienti non autosufficienti (provv. 25 gennaio 2018, n. 29, doc. web n. 7810766) (nota 12 aprile 2018).

In un altro caso, a seguito della trasmissione da parte di un medico di un documento recante una valutazione di impatto ai sensi dell'art. 35 del RGPD, nel quale veniva descritta la sua attività (svolgimento di visite mediche e ricerche; elaborazione e redazione di perizie e relazioni), è stato precisato che non compete all'Autorità esprimere una generale valutazione in merito alle scelte organizzative del titolare del trattamento, al di fuori di quanto specificamente previsto dal RGPD nel-

l'ambito della consultazione preventiva, ove ne ricorrano i presupposti (art. 36 del RGPD). È stato, altresì rappresentato che, nel trasmettere la documentazione all'Autorità, vanno specificati gli ambiti del trattamento che presentino ancora un rischio elevato nonostante le misure specificamente individuate e descritte dal titolare per i quali si richiede il parere al Garante.

Ove, invece, dalla valutazione dell'impatto dei trattamenti sulla protezione dei dati personali, non emergano rischi non adeguatamente e ragionevolmente attenuati, in conformità al principio di *accountability*, la relativa documentazione deve essere conservata in vista di eventuali controlli dell'Autorità, ma non trasmessa alla stessa (nota 13 novembre 2018).

5.4.3. I chiarimenti in relazione ai Responsabili della protezione dei dati (Rpd) e le attività con le reti dei Rpd

Alla luce del forte impatto che la nuova disciplina sul Responsabile della protezione dei dati (Rpd) determina anche nel settore sanitario, l'Ufficio ha ritenuto opportuno fornire alcuni chiarimenti in merito alla proposta pervenuta, da più realtà territoriali, di individuare un unico Rpd per tutte le strutture sanitarie di un'unica regione. Tale scelta non è, in linea di principio, contraria a quanto previsto dal RGPD; ciononostante, deve essere valutata con grande senso di responsabilità, tenendo in considerazione tutte le implicazioni tecniche, giuridiche e pratiche di tale decisione, nonché la circostanza che quello sanitario rappresenta uno dei settori più complessi del trattamento dei dati sulla salute.

Nella scelta di un unico Rpd devono comunque essere rispettati i requisiti richiesti dal RGPD per la suddetta designazione. Ciò con particolare riferimento alla possibilità che il Rpd agisca in piena indipendenza e autonomia (senza ricevere istruzioni e riferendo direttamente ai vertici) e al requisito della professionalità, che deve essere adeguata alla peculiare complessità del settore sanitario fortemente caratterizzato da un livello più elevato di conoscenze specialistiche. In tali casi deve essere prestata particolare attenzione agli ulteriori compiti e funzioni che il responsabile potrebbe svolgere, per prevenire situazioni di conflitto di interesse oppure inefficienze nell'adempimento delle funzioni proprie di tale figura (cfr., sul punto, par. 2.3. delle "Linee guida sui responsabili della protezione dei dati" del Gruppo Art. 29, adottate il 13 dicembre 2016, versione emendata del 5 aprile 2017 e "Nuove Faq sul Responsabile della protezione dei dati (Rpd) in ambito pubblico", doc. web n. 7322110). Le scelte del titolare relative alla designazione del Responsabile devono inoltre consentire effettivamente, sia ai titolari che alla moltitudine degli interessati coinvolti, di poter agevolmente contattare il Rpd. Ciò, in particolare, alla luce del rilevante numero di assistiti delle regioni che potrebbero, in qualità di interessati, avere l'esigenza di contattare lo stesso per l'esercizio dei propri diritti.

La delicatezza del settore e la particolare rischiosità dei trattamenti che lo caratterizzano, enfatizzata dal crescente impiego di nuove tecnologie e dal rilievo che assume nel contesto delle attività di cura l'utilizzo dei dati personali anche per finalità ulteriori (quali, ad esempio, quelle connesse alla ricerca scientifica) costituiscono, infatti, elementi che devono indurre a un'attenta riflessione circa l'opportunità della decisione di concentrare in un unico soggetto, la designazione del Rpd. Dovrà, pertanto, essere fatta un'attenta valutazione da parte delle aziende sanitarie in merito alla necessità di prevedere, sin dalla fase di selezione e designazione, un qualificato e congruo apporto di tale figura (in termini di ore effettive di lavoro) per la gestione delle attività del singolo titolare. La validità della scelta del Rpd unico dipende, infatti, anche dalla quantità di tempo che lo stesso potrà effettivamente

dedicare ad ogni titolare, ciò tenendo conto anche dell'impegno straordinario che si richiederà a tale figura nella prima fase di applicazione del RGPD, in relazione alle molteplici attività di adeguamento che le singole aziende devono intraprendere (nota 22 maggio 2018).

In merito al delicato ruolo dei responsabili della protezione dei dati nel settore sanitario e della ricerca, oltre a promuovere iniziative volte a sostenere, in generale, la pubblica amministrazione nel cambiamento in atto (incontri del 15 gennaio a Bari, presso il Teatro Petruzzelli, e il 6 aprile a Roma presso la sala convegni del Cnr, del 24 maggio 2018 a Bologna), l'Ufficio ha svolto tale attività anche attraverso una serie di incontri specifici con i responsabili della protezione dei dati del settore. Tra questi si segnalano nel corso del 2018, in particolare, l'incontro tenutosi il 5 luglio con i Rpd degli enti pubblici di ricerca avvenuto nell'ambito della Consulta dei Presidenti degli Enti pubblici di ricerca nazionali, presso il Cnr; quello del 20 settembre con istituzioni e enti di ricerca presso la Regione Lazio; quello del 6 novembre, presso la sala congressi dell'Ospedale Sant'Eugenio, con un Tavolo di confronto tra Rpd delle Aziende Sanitarie e Ospedaliere della Regione Lazio; infine, quello del 13 dicembre, presso l'Istituto Superiore di Sanità, con i Rpd degli Enti di ricerca.

5.4.4. Le attività di revisione dettate dalla disciplina di adeguamento al RGPD

Con riferimento all'attività di revisione delle autorizzazioni generali richiesta dall'art. 21, d.lgs. n. 101/2018, volta ad individuare le prescrizioni contenute nelle autorizzazioni generali già adottate che risultano compatibili con le disposizioni del RGPD – e segnatamente dell'autorizzazione n. 2 ("Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale") –, il Garante ha ritenuto che l'atto fosse privo di specifici elementi prescrittivi, essendo caratterizzato da una duplice valenza: autorizzatoria (atto legittimante il trattamento, per una serie di soggetti, in ambiti definiti: elenco dei soggetti destinatari dell'autorizzazione e delle categorie di dati e di operazioni ricomprese nell'atto, indicazione delle modalità con le quali presentare una nuova autorizzazione e efficacia temporale dell'atto) e ricognitiva dei principi generali applicabili in materia, vigenti all'epoca della sua adozione. Ciò stante, l'Autorità ha ritenuto l'autorizzazione generale n. 2/2016 priva di specifiche prescrizioni e, pertanto, che esulasse dall'ambito delle disposizioni di cui all'art. 21, comma 1, d.lgs. n. 101/2018 (provv. 13 dicembre 2018, n. 497, doc. web n. 9068972, posto in consultazione pubblica con avviso in G.U. 11 gennaio 2019, n. 9).

Con riferimento al trattamento dei dati genetici e dei dati personali effettuato per scopi di ricerca scientifica, il Garante, con il testé richiamato provvedimento generale di dicembre, ha provveduto all'attività di revisione delle autorizzazioni relative anche al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016) e a quello effettuato con i dati genetici. Con tale atto il Garante ha individuato le prescrizioni relative alle particolari situazioni di trattamento (artt. 6, par. 1, lett. *c*) e *d*), 9, par. 2, lett. *b*), e 4 nonché il capo IX del RGPD) contenute nelle autorizzazioni generali compatibili con le disposizioni del RGPD, ne ha disposto l'aggiornamento e ha avviato la prevista procedura di consultazione pubblica per acquisire osservazioni e proposte rispetto alle prescrizioni individuate con il predetto provvedimento, con specifico riguardo ai risvolti applicativi nonché agli eventuali profili di criticità riscontrabili o anche già sperimentati nel settore di riferimento.

In relazione al trattamento dei dati genetici, sono state mutuate dalla precedente autorizzazione generale le definizioni di alcuni termini di riferimento (campione

biologico, test genetico, test farmacogenetico, test farmacogenomico, test sulla variabilità individuale, *screening* genetico, consulenza genetica, informazione genetica) ed è stata introdotta la nuova definizione di “dato genetico” di cui all’art. 4, par. 1, n. 13, del RGPD.

Il predetto provvedimento ha inoltre mantenuto e, in minima parte, aggiornato alcune prescrizioni specifiche in ordine alla custodia e alla sicurezza dei dati genetici e dei campioni biologici, fermo restando, alla luce del nuovo quadro normativo (in particolare l’art. 32 del RGPD), l’obbligo per i titolari di mettere in atto misure tecniche e organizzative sempre adeguate e costantemente aggiornate in riferimento alle diverse variabili che caratterizzano il contesto del trattamento.

In relazione alle informazioni che devono essere fornite agli interessati, è stato previsto che anche i Mmg e i Pls evidenzino l’eventuale trattamento di dati genetici, mentre è rimasto per lo più invariato il paragrafo relativo alle consulenze genetiche e all’attività di informazione, atteso che, come per il passato, risulta indispensabile assicurare l’effettiva autodeterminazione informativa degli interessati e tutelarne la dignità.

Per quanto concerne, invece, il trattamento di dati genetici per finalità di ricerca scientifica e statistica, è stato previsto che, nel caso di impossibilità nell’acquisizione del consenso per la conservazione e l’ulteriore utilizzo di campioni biologici e di dati genetici raccolti per la realizzazione di progetti di ricerca e indagini statistiche, diversi da quelli originari, il trattamento è consentito solo se una ricerca con analoga finalità non possa essere realizzata mediante il trattamento di dati riferiti a persone dalle quali può essere o è stato acquisito il consenso informato e il programma di ricerca, oggetto di motivato parere favorevole del competente comitato etico a livello territoriale, è sottoposto a preventiva autorizzazione del Garante. Si evidenzia come tale prescrizione sia stata provvisoriamente lasciata inalterata, stante la transitorietà della fase in esame e in virtù dell’art. 22, comma 11, d.lgs. n. 101/2018.

Le prescrizioni relative ai dati riferite a minori sono state ritenute tutte compatibili, stante la particolare attenzione prestata dal RGPD ai dati personali di tali soggetti; del pari, anche la prescrizione inerente il trattamento dei dati genetici delle persone defunte, è stata ritenuta compatibile con il RGPD tenuto conto che il considerando 27 consente agli Stati membri di estendere la disciplina in materia di protezione dei dati personali anche a tali categorie di interessati.

Con riferimento alle prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, di cui all’autorizzazione generale n. 9/2016, di particolare rilevanza è il preambolo del provvedimento. In tale sezione sono evidenziate le condizioni di liceità del trattamento dei dati per finalità di ricerca medica, biomedica ed epidemiologica dando particolare enfasi agli adempimenti relativi alla valutazione di impatto e alla consultazione preventiva del Garante. Con riguardo all’ambito di applicazione delle prescrizioni viene chiarito che queste ultime trovano applicazione per tutti i trattamenti di dati sulla salute per finalità di ricerca medica, biomedica ed epidemiologica a prescindere dalla circostanza che la ricerca abbia o meno una significativa ricaduta personalizzata sull’interessato. Il provvedimento in esame viene dunque a completare le condizioni di liceità del trattamento per tutte le ipotesi di trattamento disciplinate dall’art. 110 del Codice.

L’Autorità ha inoltre ritenuto che le prescrizioni contenute nel provvedimento trovano applicazione ai trattamenti effettuati per finalità di ricerca medica, biomedica ed epidemiologica, da parte dei soggetti espressamente individuati allorché il trattamento sia necessario per la conduzione di studi effettuati con dati raccolti in precedenza a fini di cura o per l’esecuzione di precedenti progetti di ricerca ovvero ricavati da campioni biologici prelevati in precedenza per finalità di tutela della

salute o per l'esecuzione di precedenti progetti di ricerca oppure allorché il trattamento sia necessario per la conduzione di studi effettuati con dati riferiti a persone che, in ragione della gravità del loro stato clinico, non sono in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso.

Con riguardo ai presupposti di liceità del trattamento, il Garante ha altresì precisato che in tutti i casi in cui non sia possibile acquisire il consenso degli interessati, sorge in capo ai titolari del trattamento l'obbligo di documentare, nel progetto di ricerca, la sussistenza delle eccezionali ragioni impeditive o gravemente pregiudizievoli rispetto al conseguimento delle finalità della ricerca, tra le quali in particolare: motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione; motivi di impossibilità organizzativa, riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile informare in relazione al numero complessivo dei soggetti che si intende coinvolgere nella ricerca produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati; motivi di salute riconducibili alla gravità dello stato clinico in cui versa l'interessato a causa del quale questi è impossibilitato a comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso.

6 La ricerca storica, scientifica e la statistica

6.1. *Dai codici deontologici alle "regole deontologiche"*

Con i provvedimenti nn. 513, 514 e 515 del 19 dicembre 2018 (doc. web n. 9069661, 9069677 e 9069637), il Garante ha verificato, ai sensi dell'art. 20, commi 3 e 4, d.lgs. n. 101/2018, la conformità al RGPD delle disposizioni dei codici di deontologia e di buona condotta contenuti negli Allegati A.2, A.3 e A.4 del decreto legislativo n. 196/2003, ridenominandole "regole deontologiche" (di seguito anche solo regole), allegate al Codice (Allegato A). Le regole approvate, il cui rispetto costituisce condizione essenziale per la liceità e la correttezza del trattamento, devono essere interpretate ed attuate alla luce dei principi sulla protezione dei dati personali introdotti dal RGPD, quali il principio di responsabilizzazione e l'approccio basato sulla valutazione del rischio.

Per quanto concerne le "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale", il Garante ha rilevato l'incompatibilità delle disposizioni contenenti i criteri per l'identificabilità dell'interessato in quanto frutto di un approccio alla valutazione del rischio più circoscritto rispetto a quello del RGPD. Non è stato inoltre confermato l'istituto dell'autorizzazione del Garante in quanto, nel nuovo quadro normativo, l'istituto risulta confinato ad un numero limitato e circoscritto di ipotesi. Valutazioni di incompatibilità sono state effettuate anche con riferimento alla disciplina dei casi di impossibilità a fornire le informazioni agli interessati e di informativa differita, atteso che l'art. 13 del RGPD non prevede alcuna forma di deroga o semplificazione agli obblighi informativi quando i dati sono raccolti presso gli interessati. È stata altresì considerata incompatibile la sezione che prevedeva la possibilità per il titolare di raccogliere dati personali presso un soggetto rispondente in nome e per conto di un altro (cd. *proxy*: art. 6, comma 4, del codice deontologico), in quanto non prevedeva, diversamente da quanto richiesto dall'art. 105, comma 3, d.lgs. n. 196/2003, le specifiche circostanze in cui tale modalità di raccolta era ammessa.

Sono state considerate non conformi anche le disposizioni che disciplinavano le comunicazioni di dati personali a ricercatori di università o a istituti o enti di ricerca a soci di società scientifiche non facenti parte del Sistema statistico nazionale e le disposizioni relative alle "Misure di sicurezza", alla luce del diverso assetto dei requisiti di liceità del trattamento e del differente approccio alla sicurezza dei dati basato sul principio di responsabilizzazione.

Sulla base dei medesimi criteri sono state riviste le disposizioni del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (All. A.4 del Codice), ora denominate "Regole deontologiche per il trattamento a fini statistici o di ricerca". Il Garante ha rilevato l'incompatibilità di tutte quelle disposizioni del decreto legislativo n. 196/2003 che individuavano condizioni di liceità del trattamento, sia di dati comuni che delle particolari categorie di dati, inclusi i dati genetici, differenti rispetto a quelle del RGPD e del Codice. Le disposizioni dedicate alla ricerca medica, biomedica ed epidemiologica sono state, da una parte, modificate al solo fine di confermare le tutele assicurate in tale contesto agli interessati, e, dall'altra, abrogate per coordinare le regole con il

provvedimento prescrittivo adottato dal Garante ai sensi dell'art. 21, d.lgs. n. 101/2018.

6.2. *La statistica*

6.2.1. Il Programma statistico nazionale

Nel 2018 il Garante si è espresso sull'Aggiornamento 2018-2019 del Programma statistico nazionale (Psn) 2017-2019, ai sensi del codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica, effettuati nell'ambito del Sistema statistico nazionale (Sistan), All. A3 al Codice, relativo a circa 243 lavori statistici svolti dall'Istat che comportano il trattamento di dati personali, sensibili e giudiziari, rappresentati nei prospetti identificativi inseriti nell'aggiornamento e in quelli modificati rispetto alla versione inclusa nel Psn 2017-2010 (parere 9 maggio 2018, n. 271, doc. web n. 9001732).

Alcuni lavori statistici non hanno ricevuto il parere favorevole del Garante, poiché ritenuti non conformi alla normativa in materia di protezione dei dati personali.

Il Sistema integrato dei registri

In primo luogo, gravi criticità sono state rilevate in relazione al lavoro IST-02270 Sistema di integrazione logico-fisica di microdati amministrativi (Sim), già oggetto di rilievi nei pareri sui precedenti Psn. Il Sim, infatti, costituisce una vera e propria infrastruttura centralizzata, nella quale vengono integrate e duplicate numerose decine di archivi amministrativi e statistici relativi alla totalità dei cittadini: attraverso i codici fiscali delle persone fisiche censite nelle diverse banche dati, tramite tecniche di *record linkage* (che consistono nell'attribuzione allo stesso soggetto di dati provenienti da diverse fonti in ragione della presenza di chiavi comuni di collegamento), viene attribuito a ciascun individuo, uno specifico codice univoco, denominato "codice Sim", determinando una vera e propria schedatura permanente, in relazione ad ogni aspetto della vita quotidiana, con gravi rischi per i diritti e le libertà degli interessati.

Analoghe, se non maggiori, preoccupazioni ha suscitato, poi, l'intenzione dell'Istat di avvalersi, per i propri lavori statistici, di un "Sistema integrato dei registri", indicato quale motivo della conservazione dei dati identificativi diretti delle fonti amministrative. I lavori statistici che dovrebbero comporre tale sistema sono: IST-02729-Registro degli Edifici e delle Unità abitative, IST-02721-Registro base degli individui delle famiglie e delle convivenze (integrazione di più di 50 fonti amministrative, anche contenenti dati sensibili), IST-02742-Registro del lavoro (integrazione di 26 fonti amministrative), IST-01382-Registro annuale su retribuzioni, ore e Costo del lavoro individuale (integrazione di quasi 20 fonti amministrative), IST-02638-Integrazione dati e registro redditi, consumi e ricchezza. In tale prospettiva risultano critici anche i lavori IST-02638 – Integrazione dati e registri dei redditi, consumi e ricchezza, e IST-02634 – Sistema informativo sull'occupazione, ove si vorrebbero integrare, su base pluriennale, non solo fonti amministrative già utilizzate a fini statistici in altre rilevazioni, ma anche dati personali, sensibili e relativi ad ogni aspetto della vita quotidiana degli individui, raccolti presso gli interessati, anche con obbligo di risposta assistito da una sanzione amministrativa (ad es., caratteristiche delle abitazioni, redditi, deprivazione materiale, percezione delle difficoltà economiche, stato di salute, tipologie di spese di consumo anche relative a visite mediche, articoli sanitari, accertamenti diagnostici, autoconsumi, luoghi d'acquisto, ecc.).

A ciò si aggiunga che in molti lavori statistici afferenti al Sistema dei registri è stata da ultimo introdotta una nuova variabile denominata "codice univoco indi-

rizzo (Cui) di residenza Sim" o "codice univoco indirizzo (Cui) di domicilio Sim" che sembrerebbe non collegabile alla protezione dei dati personali. Al riguardo, il Garante ha rappresentato, tuttavia, che l'utilizzo di tali codici, riferibili alle persone fisiche che risultano, di volta in volta, attraverso la mera consultazione di pubblici registri, intestatarie, proprietarie, residenti o titolari di attività economiche nei luoghi individuati, è idoneo a rivelare, con tecniche di *linkage* e di georeferenziazione degli indirizzi, sia i luoghi di dimora abituale, di lavoro, di studio, di abitazione e di cura, sia i legami tra individui, luoghi, enti e istituzioni, aumentando così, esponenzialmente, il patrimonio informativo riferibile all'intera popolazione e, quindi, anche i connessi rischi per le libertà e diritti degli interessati.

Pertanto il Garante, pur riconoscendo la rilevante finalità di interesse pubblico perseguita dall'Istituto nazionale di statistica, nel parere espresso – in considerazione dei predetti rischi, derivanti dall'integrazione di una moltitudine di archivi amministrativi e statistici, dalla conservazione degli identificativi diretti e dall'integrazione anche di fonti statistiche raccolte presso gli interessati con obbligo di risposta, nonché dall'indeterminatezza delle indagini e dei risultati statistici che tali trattamenti sono predeterminati a realizzare, anche attraverso la profilazione degli interessati – ha sollevato interrogativi circa la compatibilità dei predetti trattamenti con l'essenza del diritto alla protezione dei dati personali, che risulta di per sé gravemente compromesso da un tale disegno.

Ciò, anche in presenza di dati pseudonimizzati, aggregati o anonimi, in considerazione delle elevate probabilità di re-identificazione dovute all'immenso patrimonio informativo progressivamente accumulato dall'Istituto e alle tecniche di elaborazione utilizzabili.

Lavori statistici relativi al censimento permanente

Ulteriori gravi criticità, salvo quanto si dirà al punto 6.2.2, sono state evidenziate dal Garante in relazione ai lavori statistici connessi con la realizzazione del cd. censimento permanente.

Come più volte segnalato dal Garante, anche al Parlamento (segnalazione 7 novembre 2017, doc. web n. 7447536 sulla legge di bilancio 27 dicembre 2017, n. 205), i dati trattati per scopi statistici non possono essere utilizzati per altre finalità, né comportare ricadute personalizzate sugli interessati. Tale assunto costituisce un principio cardine della protezione dei dati personali nel settore statistico, costantemente richiamato anche in ambito internazionale ed europeo (cfr. il considerando n. 27 del regolamento CE n. 2009/223 sulle statistiche europee e l'art. 4 della Raccomandazione del Consiglio d'Europa n. R (97) 18 relativa alla protezione dei dati personali raccolti e trattati per scopi statistici). La predetta garanzia è, peraltro, ribadita da ultimo anche dal RGPD, ai sensi del quale la "finalità statistica implica che il risultato del trattamento per finalità statistiche non siano dati personali, ma dati aggregati, e che tale risultato o i dati personali non siano utilizzati a sostegno di misure o decisioni riguardanti persone fisiche specifiche" (cfr. considerando 162).

Il prospettato utilizzo da parte dell'Istat dei dati personali trattati nell'ambito del censimento permanente per la finalità di revisione delle anagrafi della popolazione residente, seppur contemplato dall'art. 1, comma 223, l. n. 205/2017, non è, pertanto, compatibile con i principi e le disposizioni sopra richiamati. Il Garante ha quindi ritenuto che tutti i lavori statistici connessi alla realizzazione del censimento permanente della popolazione e delle abitazioni, non fossero caratterizzati da sufficienti garanzie idonee ad assicurare la conformità alle disposizioni del Codice e del RGPD e che sarebbero potuti quindi essere avviati solo all'esito dell'esame, da parte dell'Autorità, del Piano generale del censimento, corredato da tutti gli elementi necessari a valutare compiutamente la conformità dei predetti trattamenti alla disciplina

sulla protezione dei dati personali (e, in particolare, dalla valutazione di impatto). Sulla questione, è definitivamente intervenuto il legislatore, che all'art. 22, comma 7, d.lgs. n. 101/2018, ha previsto che le modalità di restituzione dei dati censuari per la revisione delle anagrafi debbano avvenire esclusivamente in forma aggregata.

Statistica e minori

Alcuni rilievi sono stati espressi riguardo ai lavori statistici che prevedono il coinvolgimento di soggetti minori di età: il Garante ha invitato l'Istituto a valutare con estrema attenzione, anche nell'ambito di una specifica valutazione d'impatto effettuata ai sensi dell'art. 35 del RGPD, l'opportunità di trattare dati personali riferiti a tale particolare categoria vulnerabile di interessati e ad adottare appropriate garanzie (ad esempio, innalzando l'età per la quale la raccolta dei dati viene effettuata tramite *proxy* e rendendo anonimi i dati al termine del trattamento statistico per il quale sono stati raccolti). In particolare, vista la delicatezza delle informazioni rilevate presso minori, relative anche alle discriminazioni eventualmente subite in diversi ambiti (origine etnica, identità di genere, genere, religione o credo, aspetti relativi alla salute, orientamento sessuale), sono stati richiesti specifici chiarimenti sui questionari utilizzati nell'ambito del lavoro IST-02726-Indagine sulle discriminazioni, nonché alla conservazione dei dati identificativi diretti per la "creazione di un archivio per ritorni sull'argomento", prima di avviare il trattamento.

Big data

Ulteriori rilievi sono stati formulati sul prospetto IST-02589-Uso a fini statistici dei *big data*, che coinvolgono l'utilizzo di dati personali raccolti attraverso diverse fonti informative oggetto di specifici ambiti di analisi. In particolare, con riferimento alle sperimentazioni che prevedono l'utilizzo di fonti di telefonia mobile, il Garante ha sottolineato che l'utilizzo di queste informazioni comporta specifici rischi per la riservatezza e la protezione dei dati personali degli interessati, tenuto anche conto che, grazie alle nuove tecnologie e alle nuove tecniche di analisi, elaborazione e interconnessione dei dati, risulta spesso possibile (o, comunque altamente probabile) la re-identificazione di un interessato (cd. *single-out*) anche attraverso informazioni apparentemente anonime.

Disabili

Analoghi rilievi sono stati evidenziati con riguardo al lavoro statistico IST-02748-Archivio disabilità, che conferma la tendenza dell'Istat di raccogliere e integrare banche dati amministrative diverse per costituire un ennesimo grande *repository*, in questo caso, relativo alle persone con disabilità. Al riguardo, è stata rilevata l'insufficienza delle misure di garanzia indicate nel prospetto informativo che potrebbe verosimilmente determinare la violazione delle disposizioni del Codice e del RGPD e l'Istituto è stato invitato, prima di avviare il trattamento, a comunicare al Garante tutti gli elementi necessari a consentire una compiuta valutazione circa la conformità dello stesso alla disciplina sulla protezione dei dati personali corredando tali informazioni, in particolare, con la valutazione di impatto, che dovrà essere condotta ai sensi dell'art. 35 del RGPD.

Sul tema della diffusione di variabili in forma disaggregata avente ad oggetto 23 lavori statistici, consentita nei limiti di quanto previsto dal combinato disposto dell'art. 4, comma 2, del codice di deontologia e dell'art. 13 comma 3-*bis*, d.lgs. n. 322/1989, il Garante ha rilevato che in alcuni casi, diversamente da quanto previsto nei precedenti Psn, non risultasse scongiurato il rischio di re-identificazione dei singoli interessati. A tal proposito è stata ribadita la necessità che tali dati vengano diffusi rispettando i livelli di aggregazione previsti nei precedenti Psn.

Nel parere, infine, in considerazione dell'imminente applicazione del nuovo quadro giuridico europeo in materia di protezione dei dati personali, il Garante ha segnalato la necessità che l'Istat e gli altri soggetti del Sistan, in relazione all'insieme di tutti i lavori inseriti nel Psn, garantiscano la piena conformità al RGPD, in par-

ticolare, assicurando – per impostazione predefinita e fin dalla progettazione – la protezione dei dati personali nell'ambito dei trattamenti effettuati nel Psn (art. 25 del RGPD) con l'ausilio del responsabile per la protezione dei dati (artt. 37-39 del RGPD). Si è inoltre evidenziata la necessità di effettuare una valutazione di impatto sulla protezione dei dati tenuto conto che nello schema di aggiornamento sono ricompresi numerosi lavori statistici che presentano un elevato rischio per i diritti e le libertà degli interessati. Sempre con riferimento ai profili di adeguamento al Regolamento, è stata evidenziata la necessità di fornire agli interessati tutte le informazioni previste dagli artt. 13 e 14 del RGPD, necessarie a garantire un trattamento corretto e trasparente.

6.2.2. Il censimento permanente

In seguito ai rilievi critici espressi nel citato parere sul Psn, l'Istat ha trasmesso all'Autorità una nuova versione del Piano Generale di Censimento, corredata della relativa valutazione di impatto. Il Garante, con provvedimento del 4 ottobre 2018, n. 459 (doc. web n. 9047672), reso ai sensi dell'art. 2-*quinquesdecies* del Codice relativo ai trattamenti che presentano rischi elevati per l'esecuzione di un compito di interesse pubblico, come quelli relativi al censimento permanente, ha dato la sua autorizzazione all'avvio della prima fase del menzionato censimento.

Riservandosi di esprimersi sulle fasi successive, il Garante, nell'autorizzare l'avvio della prima fase del censimento, ha espressamente richiesto che, anche per le famiglie inserite nell'indagine cd. porta a porta, venissero espressamente previste modalità alternative alla raccolta *de visu*, in modo da assicurare le medesime garanzie di riservatezza previste per chi invece riceverà a casa la lettera dell'Istat, a cui è possibile rispondere anche dal pc o al telefono. Ciò per evitare che l'obbligatoria presenza fisica del rilevatore, a cui, in caso di rilevazione *de visu*, è necessario fornire direttamente le risposte, possa comportare disagi per gli interessati, soprattutto nelle piccole comunità, con una maggiore ingerenza nella sfera privata degli stessi (si pensi ai casi di soggetti vulnerabili o timorosi, anziani e persone malate), i quali si troverebbero a dover fornire ad un soggetto estraneo numerose e dettagliate informazioni relative alla propria famiglia e abitazione, a pena di sanzione.

6.2.3. Parere sullo schema di Linee guida per l'accesso a fini scientifici ai dati elementari del Sistan

Il Garante si è espresso sullo schema di Linee guida per l'accesso a fini scientifici ai dati elementari del Sistan (provv. 21 giugno 2018, n. 388, doc. web n. 9023239), elaborato da Comstat per dare attuazione alla disciplina di cui all'art. 5- *ter*, d.lgs. 14 marzo 2013, n. 33. Nelle Linee guida sono state recepite le indicazioni fornite dall'Ufficio al fine di assicurare che i trattamenti di dati personali effettuati per consentire l'accesso a fini scientifici di dati elementari statistici siano conformi al nuovo Regolamento europeo.

L'accesso a fini scientifici potrà riguardare dati elementari a cui sono stati applicati metodi di controllo per la tutela della riservatezza (*file* MFR), ovvero dati a cui non sono stati applicati tali metodi esclusivamente nell'ambito di appositi laboratori.

Le Linee guida sottoposte al parere del Garante stabiliscono, in primo luogo, i criteri oggettivi e soggettivi e la procedura per il riconoscimento delle organizzazioni che possono essere prese in considerazione per il riconoscimento quale "Ente di ricerca", come università ed enti di ricerca, nonché istituzioni pubbliche o private, o loro strutture interne di ricerca, nel caso in cui l'organizzazione interna risulti

improntata al principio di separazione tra le strutture gestionali e amministrative e quella che svolge l'attività di ricerca, che deve essere contraddistinta da autonomia nelle conclusioni scientifiche.

Una specifica sezione è poi dedicata alle caratteristiche del progetto di ricerca, soggetto al vaglio da parte dell'ente Sistan che intende concedere l'accesso ai dati elementari. Occorre in tal caso verificare se lo scopo perseguito risulta pertinente rispetto alle finalità di ricerca e se sia chiaramente motivata l'impossibilità di conseguire lo scopo della ricerca con dati anonimi.

L'ente Sistan deve altresì verificare l'interesse pubblico e i benefici attesi, in termini di conoscenza, perseguiti con la ricerca e tenere conto della facilità di accesso ai risultati della ricerca e dell'ampiezza della loro diffusione.

Il progetto, nel caso di richiesta di *file* MFR, deve recare anche la descrizione dei metodi impiegati per l'analisi dei dati con l'indicazione delle misure tecniche e organizzative adottate per garantirne la sicurezza in tutte le fasi del trattamento.

Per quanto riguarda l'elaborazione del *file* FMR da parte dell'ente Sistan, le Linee guida prevedono che i criteri di protezione statistica siano stabiliti a seguito di una valutazione d'impatto sulla protezione dei dati finalizzata a determinare i rischi per i diritti e le libertà delle unità statistiche, tenuto conto dell'eventuale coesistenza di rilasci di altri *file* di dati elementari che contengono dati riferiti alla stessa unità statistica o di altre fonti liberamente accessibili, considerato che dal confronto tra più *dataset* potrebbero ottenersi informazioni sui rispondenti, tali da invalidare le misure di protezione adottate.

Le Linee guida prevedono inoltre specifiche e ulteriori garanzie per le particolari categorie di dati personali di cui agli artt. 9 e 10 del RGPD, in base alle quali, pur in presenza di un rischio solo residuale di re-identificazione dei rispondenti, devono essere adottate apposite tecniche, quali la casualizzazione, per assicurare l'anonimia delle variabili riservate.

L'accesso, invece, ai dati elementari a cui non sono applicati metodi di controllo per la tutela della riservatezza può essere accordato dall'ente Sistan solo nell'ambito di appositi ambienti fisici/virtuali (laboratori), a condizione che, nella richiesta, siano motivate la necessità di tale accesso e l'impossibilità di conseguire altrimenti i risultati della ricerca (art. 5-*ter*, comma 2, d.lgs. n. 33/2013).

Con riguardo ai criteri di accreditamento per la gestione dell'accesso da remoto, lo schema di linee guida prevede che, ai fini dell'accreditamento, l'ente Sistan deve effettuare una valutazione dell'idoneità del soggetto che intende accedere ai dati da remoto. Ciò impone, in particolare, la valutazione dello scopo scientifico perseguito dal soggetto da accreditare, dell'adeguatezza della propria struttura organizzativa e delle misure adottate per la gestione e la sicurezza dei dati.

In merito alle caratteristiche del cd. punto di accesso da remoto, tuttavia, il Garante ha evidenziato una residuale criticità relativa alle misure tecniche e organizzative che devono assicurare la sicurezza, anche fisica, della postazione di lavoro per l'accesso ai dati statistici effettuati da remoto. È stato ritenuto necessario, infatti, che i punti di accesso da remoto siano collocati in locali dedicati, ai quali possano accedere i soli ricercatori autorizzati, con registrazione degli accessi fisici.

Le Linee guida prevedono, infine, che l'ente Sistan debba assumere specifici provvedimenti nei confronti del soggetto abilitato a rappresentare l'Ente di ricerca riconosciuto, del ricercatore responsabile del progetto, del referente per l'utilizzo dei dati elementari nonché di ogni ricercatore che abbia agito in violazione degli impegni assunti tramite la specifica documentazione sottoscritta e allegata alla domanda di riconoscimento e alla proposta di ricerca. Ciò ferme restando le sanzioni amministrative per i casi di violazione del divieto di effettuare trattamenti dei dati elemen-

tari diversi da quelli previsti nel progetto di ricerca, di conservare i dati elementari oltre i termini di durata del progetto, di comunicare i medesimi dati a terzi e di diffonderli (art. 5-*ter*, comma 1, lett. *c*), d.lgs. n. 33/2013), nonché le altre sanzioni stabilite in caso di violazione delle disposizioni in materia di protezione dei dati personali dalla normativa di settore, le sanzioni previste dal codice civile e dal codice penale.

7 I trattamenti in ambito giudiziario e da parte di Forze di polizia

7.1. *I trattamenti in ambito giudiziario*

Trattamento dati da parte di ausiliari del giudice

Con riferimento al trattamento dei dati da parte di ausiliari del giudice, il Garante ha affermato di non avere competenza in merito a tali trattamenti dovendo la richiesta di valutazione essere rivolta all'autorità giudiziaria. Sia il RGPD (art. 55, par. 3), sia il Codice (art. 154, comma 7, come modificato dal decreto legislativo n. 101/2018) dispongono che l'autorità di controllo, quale appunto il Garante, non è competente per il controllo dei trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni, tra le quali rientra anche l'attività degli ausiliari del giudice (cfr. artt. 191 e ss. c.p.c.). Ciò in linea con l'orientamento già espresso prima dell'entrata in vigore del RGPD, da riferire al principio costituzionale di separazione dei poteri, secondo cui i trattamenti di dati personali effettuati presso l'autorità giurisdizionale rientrano tra quelli compiuti per motivi di giustizia, in relazione ai quali le norme a tutela della protezione dei dati personali trovano limitata applicazione.

In questa linea, costante giurisprudenza conferma che la questione relativa a presunte omissioni o irregolarità della Ctu attiene a valutazioni di competenza del giudice in merito alla "violazione del principio del contraddittorio e conseguente pregiudizio del diritto di difesa delle parti" la cui incidenza sul contenuto della consulenza e sulle relative conclusioni finali "deve essere dedotta con onere a carico del ricorrente" (cfr. *ex plurimis* Cass. civ., sez. II, 14 febbraio 2017, n. 3893; v. pure Cass. civ., sez. II, 5 gennaio 2011, n. 234, che ha cassato la sentenza di merito con la quale era stato liquidato il compenso al Ctu nonostante la declaratoria di nullità della consulenza per violazione del principio del contraddittorio). In particolare, la segnalante ha lamentato il rifiuto del Ctu di comunicarle i dati sulla salute del padre della figlia, contenuti nei test psicodiagnostici effettuati ai fini dell'elaborazione della relazione peritale oggetto di valutazione da parte del giudice per il decreto di affidamento della minore. L'Autorità, pur nella consapevolezza della delicatezza della tematica, perché riguardante l'interesse di una minore, richiamando tali principi e, in particolare, in ragione della pendenza del termine di impugnazione del decreto di affidamento adottato sulla base della relazione peritale, ha archiviato la segnalazione (nota 30 novembre 2018).

7.2. *I trattamenti da parte di Forze di polizia*

Per quanto riguarda i trattamenti effettuati dalle Forze di polizia, l'attività si è concentrata anzitutto sull'attuazione delle direttive n. 680/2016 e 681/2016; da segnalare anche gli scambi intercorsi con il competente Dipartimento del Ministero dell'interno in relazione ai lavori dell'*Europol Coordination Board* per ottenere i dati di contatto dell'autorità nazionale competente per l'esercizio del diritto di accesso a Europol da parte degli interessati. Similmente, contatti sono stati presi con il menzionato Ministero anche per quanto riguarda l'esercizio dei diritti degli interessati da parte dei richiedenti asilo dei quali vengono acquisite le impronte digitali.

"SARI Enterprise"

Il Garante ha effettuato accertamenti in merito ad un progetto del Ministero dell'interno relativo alla realizzazione di un sistema automatico di ricerca di un volto

presente nell'archivio dei soggetti foto-segnalati, denominato "SARI Enterprise".

Il trattamento dei dati biometrici ricavabili dall'immagine facciale, effettuato dalle Forze di polizia a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, è previsto e disciplinato da una pluralità di fonti normative (art. 4 del Tulps, approvato con r.d. 18 giugno 1931, n. 773 e art. 7 del relativo regolamento di esecuzione, approvato con r.d. 6 maggio 1940, n. 635; art. 349 c.p.p.; art. 11, d.l. 21 marzo 1978, n. 59, convertito in legge 18 maggio 1978, n. 191; art. 5, d.lgs. 25 luglio 1998, n. 286; decreto del Ministro dell'interno 24 maggio 2017, recante l'individuazione dei trattamenti di dati personali effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'art. 53, comma 3, del Codice).

Con i sistemi attualmente in uso, l'attività di ricerca della presenza di un soggetto nell'archivio delle persone foto-segnalate avviene tramite l'operazione manuale di un operatore idonea ad inserire, nei campi presenti nella maschera di interrogazione dell'archivio, informazioni anagrafiche, connotati e contrassegni (ad es., colore dei capelli, degli occhi, tatuaggi).

Il progettato sistema "SARI Enterprise" non effettua elaborazioni aggiuntive rispetto al passato, limitandosi ad automatizzare alcune operazioni in vista dell'effettuazione della ricerca nel *database* dei soggetti foto-segnalati attraverso l'inserimento di una immagine fotografica elaborata automaticamente al fine di fornire l'elenco di foto segnaletiche somiglianti, ottenute attraverso un algoritmo decisionale che ne individua la priorità, dalla più alla meno somigliante.

Per tali ragioni, secondo il Garante l'utilizzo del sistema "SARI Enterprise" non costituisce un nuovo trattamento di dati personali, ma una nuova modalità di trattamento di dati biometrici, che dovrà comunque essere effettuata nel rispetto delle regole previste dalla normativa rilevante in materia di tutela dei dati personali.

Né il trattamento in esame incorre nel divieto di cui all'art. 8, d.lgs. 18 maggio 2018, n. 51, relativo alle decisioni fondate unicamente su un trattamento automatizzato, compresa la profilazione, basate sulle categorie particolari di dati personali di cui all'art. 9 del RGPD (tra le quali rientrano i dati biometrici ricavabili dall'immagine facciale), in quanto il trattamento in argomento costituisce un mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione da parte dell'operatore di polizia di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema. Sulla base di tali elementi il Garante ha ritenuto che il trattamento di dati personali da realizzarsi mediante il sistema "SARI Enterprise" non presenta criticità sotto il profilo della protezione dati (provv. 26 luglio 2018, n. 440, doc. web n. 9040256).

Videosorveglianza in mobilità

Il Garante ha effettuato una verifica preliminare su un sistema di "videosorveglianza in mobilità" da porre in dotazione al personale della Polizia penitenziaria. Il sistema è composto dai sottosistemi "Scout" (dispositivo veicolare) ed "Explor" (dispositivo personale). L'apparato "Scout" permette all'operatore di effettuare la videoripresa attraverso telecamere montate sul mezzo e di trasmettere i filmati, in tempo reale, alla centrale operativa competente per lo svolgimento del servizio. Il dispositivo è dotato di telecamera frontale, per la videoripresa delle immagini, nonché di una batteria integrata, ed è inoltre concepito per l'utilizzo portatile da parte dell'operatore. L'apparato "Explor", invece, è un dispositivo mobile in dotazione all'operatore di polizia penitenziaria, utilizzato come equipaggiamento personale, al fine di fornire allo stesso uno strumento di videoripresa funzionale alla documentazione delle attività svolte in occasione di particolari circostanze operative. I sistemi non sono dotati di *software* per il riconoscimento facciale.

L'utilizzo del sistema di videosorveglianza dinamica è previsto, principalmente, nel corso di attività di traduzione di detenuti e piantonamenti o all'interno delle sezioni detentive degli istituti penitenziari.

Il Garante ha rilevato che l'acquisizione delle immagini relative allo svolgimento delle attività istituzionali della Polizia penitenziaria nei contesti indicati appare rivolta alla tutela dell'ordine e sicurezza interna degli Istituti penitenziari, alla sicurezza delle traduzioni e alla prevenzione o repressione di reati in atto o consumati. In particolare, i contesti e luoghi di utilizzo in cui è limitato l'impiego del sistema appaiono senz'altro caratterizzati da situazioni che espongono gli operatori della polizia penitenziaria ed i terzi coinvolti a potenziali pericoli per l'incolumità e la sicurezza. Pertanto, l'acquisizione e la registrazione di videoriprese nei casi individuati nel disciplinare appare, in termini generali, legittima e rispettosa dei principi di necessità e proporzionalità.

Il Garante, tuttavia, ha prescritto di limitare l'impiego dei sistemi di videosorveglianza a situazioni di effettiva necessità, per prevenire un pericolo o per altra concreta ed individuata esigenza che non possa essere altrimenti soddisfatta, prevedibile o sopraggiunta nel corso dello svolgimento delle attività istituzionali. Ciò, in particolare, vale per le perquisizioni, per le quali si richiede una maggiore precisione nel distinguere le esigenze ordinarie da quelle straordinarie. Si è segnalata altresì l'esigenza di specificare meglio la previsione relativa alla possibilità di effettuare controlli di persone o veicoli che, per quanto riguarda quelli non aventi finalità investigativa, non deve consentire riprese di situazioni che non presentino concreta necessità di acquisire immagini.

In caso di utilizzo del sistema "Explor" all'interno delle aule di tribunale, l'autorizzazione dovrà essere richiesta al giudice monocratico o al presidente del collegio. L'informativa ai terzi in ordine alla registrazione nei predetti luoghi per motivi di sicurezza dovrebbe essere resa o dalla medesima autorità giudiziaria, o dalla polizia penitenziaria su delega espressa del giudice.

La conservazione delle immagini che non diano evidenza di eventi rilevanti è limitata ad un periodo di sette giorni, necessario a verificarne il contenuto. In ordine alla prevista conservazione per 120 giorni delle "immagini relative a fatti non costituenti reato, ma rilevanti per l'ordine e la sicurezza pubblica degli Istituti o delle camere di sicurezza site presso tribunali e ospedali", è parso opportuno che siano precisate le condizioni al ricorrere delle quali è ammessa la conservazione delle immagini per tale periodo prolungato.

Subordinatamente al recepimento delle osservazioni sopra riportate, il Garante non ha ravvisato elementi ostativi all'impiego dei sistemi di videosorveglianza in mobilità Scout ed Explor da parte del personale della Polizia penitenziaria (provv. 5 aprile 2018, n. 196, doc. web n. 8577214).

Database nazionale degli operatori della sicurezza privata

Il Ministero dell'interno ha chiesto al Garante un parere in merito alla conformità alla disciplina rilevante in materia di tutela dei dati personali del disciplinare recante le procedure per l'accreditamento al *database* nazionale degli operatori della sicurezza privata.

Il *database*, di prossima attivazione, è previsto dall'art. 252-*bis*, r.d. 6 maggio 1940, n. 635, recante "Approvazione del regolamento per l'esecuzione del testo unico 18 giugno 1931, n. 773, delle leggi di pubblica sicurezza", introdotto dall'art. 1, comma 1, lett. *e*), d.P.R. 4 agosto 2008, n. 153, in base al quale: "Le guardie particolari sono iscritte in un apposito registro della prefettura, nel quale sono annotati gli istituti e gli altri soggetti presso cui prestano o hanno prestato servizio e tutte le variazioni relative al rapporto di servizio, la formazione acquisita, l'impiego prevalente nell'anno, nonché, succintamente, i motivi di cessazione dal servizio".

Il *database* è volto ad agevolare le attività di controllo amministrativo delle prefetture, competenti a rilasciare i titoli autorizzatori previsti dalle vigenti normative, nonché delle questure, a loro volta competenti ad esercitare la sorveglianza sui servizi di vigilanza privata.

Il *database* contiene esclusivamente gli elementi essenziali riguardanti il rilascio dei titoli di approvazione della nomina a guardia giurata e le vicende concernenti tali titoli autorizzatori (concessione, revoca, sospensione etc.) e non reca "dati di polizia" relativi agli accertamenti finalizzati all'adozione dei provvedimenti di concessione e revoca del decreto di approvazione della nomina a guardia giurata. Atteso che il trattamento non risulta effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, esso rientra nel campo di applicazione del RGPD.

Il Garante ha rilevato, tuttavia, che non risultano previste misure tecniche e organizzative pienamente soddisfacenti per garantire un livello di sicurezza adeguato al rischio connesso al trattamento e volte ad assicurare la protezione dei dati trattati fin dalla progettazione e per impostazione predefinita. Ulteriormente, fermo restando il principio della *accountability*, il Ministero è stato invitato a valutare l'adozione delle seguenti cautele: prevedere il tracciamento di tutte le operazioni effettuate sui dati personali, tali da consentire l'identificazione del soggetto che ha effettuato l'accesso o altra operazione di trattamento e la data ed ora in cui il trattamento è stato effettuato. In tale contesto, si è segnalata l'esigenza di dettare una specifica disciplina della conservazione dei *file* di *log*; prevedere il rilascio, agli incaricati del trattamento, delle istruzioni in merito alle modalità ed all'ambito del trattamento consentito; modificare periodicamente la *password*, ad esempio almeno ogni sei mesi; non assegnare il codice per l'identificazione, laddove utilizzato, ad altri incaricati, neppure in tempi diversi; disattivare le credenziali di autenticazione non utilizzate da un determinato periodo di tempo (es. almeno sei mesi), salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; disattivare le credenziali anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali; impartire istruzioni a coloro che agiscano sotto l'autorità del titolare di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento; verificare periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione; proteggere i dati personali contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies*, c.p., mediante l'attivazione di idonei strumenti elettronici, da aggiornare con cadenza almeno semestrale; effettuare, almeno annualmente, gli aggiornamenti periodici dei programmi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti; adottare idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni (provv. 11 luglio 2018, n. 415, doc. web n. 9054325).

7.3. *Il controllo sul Sistema di informazione Schengen*

Il Sistema d'informazione Schengen (SIS II) permette alle autorità nazionali doganali, di polizia e di controllo delle frontiere di scambiarsi agevolmente informazioni sulle persone che potrebbero essere coinvolte in reati gravi. Con l'eliminazione dei controlli alle frontiere interne, il SIS II svolge un ruolo essenziale nel facilitare la libera circolazione delle persone nello spazio Schengen. Nel Sistema sono inoltre contenute anche segnalazioni sulle persone scomparse, soprattutto minori, e infor-

mazioni su determinati beni, quali banconote, automobili, furgoni, armi da fuoco e documenti di identità che potrebbero essere stati rubati, sottratti o smarriti.

È tuttora in corso l'attuazione delle raccomandazioni ricevute in esito alla valutazione sui trattamenti di dati personali effettuati in applicazione dell'*Acquis* di Schengen svoltasi nel 2016 (cfr. Relazione 2017, p. 80).

Come noto, il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nel SIS II, in virtù dei quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale dell'archivio Schengen, ossia al Dipartimento della pubblica sicurezza (cd. accesso diretto). Al riguardo, condividendo la raccomandazione formulata all'esito della precedente valutazione sull'applicazione dell'*Acquis* di Schengen, il Ministero invia trimestralmente *report* statistici, privi di informazioni di natura personale, contenenti dati idonei a monitorare le richieste degli interessati e l'attività di riscontro compiuta dalla Divisione NSIS.

Anche se il numero delle richieste degli interessati che ancora pervengono direttamente al Garante ha subito un lieve calo rispetto agli anni precedenti, tra queste sono in lieve aumento quelle di interessati i quali lamentano un insoddisfacente od erroneo riscontro alle loro richieste da parte della autorità nazionale di polizia e, pertanto, chiedono l'intervento del Garante al fine di vederle soddisfatte.

Infine si continua ad assistere ad un moderato ma costante aumento delle richieste di accesso da autorità nazionali di controllo di altri Stati, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane. Le relative informazioni vengono comunicate, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni di cui all'art. 62 della decisione 2007/533/GAI del Consiglio e all'art. 46 del regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio.

8 L'attività giornalistica

Grande attenzione ha continuato ad essere dedicata ai profili legati alla libertà di manifestazione del pensiero. Non sono mancati infatti reclami e segnalazioni volti a lamentare lesioni del diritto alla riservatezza ad opera degli organi di informazione, anche per effetto della diffusione delle notizie diffuse sulla rete e sui *social media*.

Nell'affrontare tali questioni, il Garante ha dovuto ricercare, di volta in volta, il punto di equilibrio che, in concreto, assicurasse un adeguato bilanciamento tra la libertà di informazione e il diritto ad essere informati, da un lato, e la protezione dei dati personali, dall'altro.

In numerose occasioni, le interlocuzioni istruttorie con i titolari coinvolti sono state sufficienti a conseguire l'obiettivo richiesto dall'interessato, in quanto ad esse hanno fatto seguito interventi spontanei di rimozione dei contenuti ritenuti lesivi dagli interessati o la deindicizzazione (cd. *delisting*) degli Url, oggetto di reclamo, dai risultati restituiti dai principali motori di ricerca.

Nei casi in cui ciò non è avvenuto, l'Autorità ha dovuto avviare formali istruttorie che si sono concluse con provvedimenti di accoglimento o di rigetto e che hanno riguardato diverse tematiche delle cui principali si dà sintetico conto di seguito.

Diffusione di dati personali sui *social network*

Numerosi reclami e segnalazioni hanno avuto ad oggetto la pubblicazione di dati personali ritenuti lesivi (commenti, fotografie, ecc.) sui profili *social* e, soprattutto, su Facebook.

Nella maggior parte dei casi, come accennato, a seguito di una prima richiesta di informazioni inviata dall'Autorità, il titolare del trattamento si è adeguato spontaneamente alle istanze dell'interessato rimuovendo i contenuti segnalati. Negli altri casi, le decisioni assunte dal Garante si sono andate consolidando in una serie di orientamenti.

Fra questi merita menzionare, ad esempio, l'ordine impartito alla piattaforma di provvedere all'eliminazione delle foto di minori postate da uno dei due genitori separati senza il consenso dell'altro, o delle foto e video ritraenti un terzo in dissenso con tale pubblicazione (in materia v. pure le decisioni di merito del Tribunale di Mantova 19 settembre 2017 e del Tribunale di Roma, sez. I civ., ord., 23 dicembre 2017).

Alcune segnalazioni hanno riguardato la pubblicazione di dati personali (nomi, immagini, numeri di cellulari) all'interno di siti pornografici (prevalentemente registrati fuori dall'UE).

Numerosi continuano ad essere i casi che, dichiaratamente volti a segnalare presunte violazioni del trattamento dei dati personali, sono risultati espressione di altre fattispecie (anzitutto la diffamazione) non esaminabili dal Garante.

Delisting

Numerose sono state anche le istanze pervenute all'Autorità, volte ad ottenere l'aggiornamento o la rimozione di dati, inizialmente trattati in modo lecito, in ragione di una modifica delle situazioni originarie o del trascorrere del tempo, in applicazione del principio affermato dalla sentenza della Corte di giustizia C-131/12 del 13 maggio 2014, "Google Spain e inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González", e ora riconosciuto esplicitamente anche dall'art. 17 del RGPD "Diritto alla cancellazione (diritto all'oblio)".

La maggior parte dei reclami presentati in tale prospettiva ha avuto ad oggetto richieste di rimozione di Url rivolte nei confronti di Google inc., mentre solo un

numero esiguo ha riguardato altri motori di ricerca (Bing, Yahoo, Virgilio). La frequenza dei reclami volti ad ottenere il cd. *delisting* sembra essere il segno della sempre più diffusa consapevolezza degli effetti negativi che la permanenza sul web di alcune notizie può comportare nella sfera personale dell'individuo, anche ai fini della definizione delle sue relazioni con il mondo esterno.

A questo riguardo, la maggior parte dei reclami pervenuti si è risolta con un'adesione spontanea da parte del titolare del trattamento alle richieste del reclamante, a seguito dell'avvio dell'istruttoria preliminare.

Nel merito, la maggior parte delle richieste di rimozione di Url è stata respinta, essendo stato ritenuto prevalente l'interesse del pubblico ad avere accesso alle informazioni in questione. Questo è stato, ad esempio, il caso di notizie rinvenibili sul web non particolarmente risalenti, come quelle riguardanti un procedimento penale, non ancora definito, per evasione fiscale iniziato nel 2014 e il conseguente sequestro preventivo effettuato nel 2016 sui conti bancari intestati all'interessato (provv. 13 dicembre 2018, n. 503, doc. web n. 9075202). In altri casi, le ragioni dell'interessato sono state considerate recessive rispetto al diritto di informazione in quanto relative a condanne per reati gravi, tali da poter avere riflessi sull'attività professionale svolta. È quanto avvenuto, ad esempio, per alcuni articoli di stampa relativi ad un procedimento penale conclusosi, nel novembre 2005, con la condanna per il reato di violenza sessuale aggravata, resa definitiva per effetto della pronuncia della Corte di cassazione nel luglio 2007 (provv. 13 dicembre 2018, n. 505, doc. web n. 9075345); o, ancora, concernenti un personaggio con un ruolo pubblico (imprenditore e corrispondente consolare nelle isole dei Caraibi) (provv. 13 dicembre 2018, n. 506, doc. web n. 9075357).

Un provvedimento di accoglimento parziale è stato invece adottato su ricorso dell'interessato nei confronti di una società editrice e del gestore di un motore di ricerca al fine di ottenere l'inibizione della reperibilità in rete di due articoli, uno dei quali relativo a circostanze alle quali il ricorrente era estraneo – come dimostrato dall'assenza, all'interno di esso, di informazioni a lui riferibili – e l'altro riguardante una vicenda giudiziaria, ormai risalente nel tempo, nella quale era stato coinvolto nel 2001. Detto ricorso, in effetti, non essendosi ancora concluso il relativo procedimento alla data a partire dalla quale ha trovato applicazione il RGPD, è stato esaminato come reclamo, essendo venuta meno l'applicabilità delle norme del decreto legislativo n. 196/2003 relative alla disciplina dei ricorsi. Il Garante ha dichiarato il reclamo inammissibile nei confronti della società convenuta, essendo risultata erroneamente citata quale editrice degli articoli in questione (pur prendendo atto dell'adesione spontanea manifestata dall'effettivo titolare) e lo ha invece parzialmente accolto nei confronti del gestore del motore di ricerca in ragione del tempo decorso e della frammentarietà delle informazioni presenti all'interno della pagina correlata all'Url di cui era stata chiesta la rimozione (provv. 13 dicembre 2018, n. 502, doc. web n. 9073755). Le decisioni favorevoli si sono invece incentrate, soprattutto, su vicende processuali risalenti e conclusesi con l'archiviazione, o comunque per le quali l'interesse pubblico all'informazione è risultato affievolito.

Violenza sessuale

L'Autorità, a seguito dell'avvenuta diffusione da parte di alcune reti televisive e di varie testate giornalistiche di servizi ed articoli riportanti informazioni dettagliate idonee ad identificare, sia pure indirettamente, la vittima di una violenza sessuale – quali, in particolare, la nazionalità e la professione svolta dalla medesima, oltreché la via ed il nome dell'esercizio commerciale nel quale si era consumato l'evento – ha dovuto adottare in via d'urgenza, nei confronti dei titolari del trattamento, alcuni provvedimenti di limitazione dell'ulteriore diffusione di detti dati, ai sensi dell'art. 58, par. 2, lett. *f*), del RGPD. Il Garante ha infatti ribadito la necessità di garantire,

fermo restando il limite dell'essenzialità dell'informazione rispetto a fatti di interesse pubblico, particolari forme di tutela alle vittime di gravi reati, conformemente a quanto stabilito anche da altre disposizioni ordinamentali, quali quelle contenute nel codice di procedura penale. Conclusa l'istruttoria, nel corso della quale i titolari del trattamento coinvolti hanno fornito idonee assicurazioni in ordine all'avvenuta adozione delle misure volte ad inibire l'ulteriore divulgazione dei dati indicati, il Garante, anche al fine di consolidare gli effetti già prodotti dai citati atti di limitazione, ha adottato altrettanti provvedimenti di divieto di tale trattamento estendendolo anche a servizi o ad articoli ulteriori rispetto a quelli già individuati (provv.ti 29 novembre 2018, n. 486, doc. web n. 9065775; n. 487, doc. web n. 9065782; n. 488, doc. web n. 9065793; n. 489, doc. web n. 9065800; n. 490, doc. web n. 9065807).

Foto segnaletiche

L'Autorità è tornata ad occuparsi della diffusione di foto segnaletiche da parte degli organi di informazione a seguito di segnalazioni pervenute anche nel periodo in esame.

Ribadendo una posizione espressa più volte in passato, il Garante ha ricordato che la diffusione di foto segnaletiche, non giustificata da comprovate necessità di giustizia e di polizia, costituisce un trattamento illecito di dati personali ed ha precisato che l'illiceità non viene meno nel caso in cui le immagini siano raccolte nel corso di conferenze stampa delle Forze di polizia.

Proprio con riferimento alla diffusione di dati e immagini da parte delle Forze dell'ordine, e sulla scia di un dialogo aperto con i vertici di queste ultime, il Garante in una lettera al Capo della polizia di Stato del giugno 2018 ha stigmatizzato la prassi perdurante di esibire ai giornalisti tali fotografie evidenziando la peculiare criticità del web che, attraverso l'associazione, rispetto a ciascuna foto segnaletica, del nome e cognome della persona ritratta (cd. taggatura), favorisce una circolazione della stessa senza limiti geografici e temporali e, di fatto, una "schedatura permanente" dell'interessato.

Su tale tema il Garante ha adottato un provvedimento in seguito ad un reclamo con cui l'interessato chiedeva la rimozione di articoli di stampa che riportavano la notizia del suo arresto quale presunto "responsabile di tentato furto archeologico e danneggiamento" di un sito archeologico, diffondendo i suoi dati anagrafici e riportando altresì la sua foto segnaletica.

Il Garante, ritenendo che la pubblicazione delle fotografie segnaletiche fosse illecita, in quanto non risultava essere supportata da comprovate ragioni di giustizia e di polizia né altrimenti giustificata in ragione di esigenze informative sulla vicenda, ha accolto il reclamo (provv. 7 febbraio 2019, n. 38, doc. web n. 9101651).

Verifica di conformità del codice deontologico

Si è proceduto alla verifica di compatibilità con il RGPD del codice deontologico dei giornalisti prevista dall'art. 20, comma 4, d.lgs. n. 101/2018. Nell'ambito di tale verifica si è provveduto ad identificare le disposizioni ritenute compatibili con il RGPD al fine di disporne la pubblicazione in Gazzetta ufficiale con la nuova denominazione di "Regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica", avvenuta il 4 gennaio 2019. In tale occasione si è altresì provveduto ad aggiornare la lettura dei richiami ad atti normativi, da ritenersi ormai superati (come ad es. la legge n. 675/1996), contenuti nel codice deontologico, evidenziando l'opportunità di integrare la lettura di alcune disposizioni ivi contenute alla luce delle modifiche normative rilevanti introdotte nella disciplina di specie, quali l'inserimento dei dati biometrici e genetici tra le categorie di dati particolari. Tali disposizioni costituiscono condizioni essenziali di liceità del trattamento di dati in ambito giornalistico e conserveranno la loro efficacia sino alla revisione delle stesse in collaborazione con il Consiglio nazionale dell'ordine dei giornalisti, secondo quanto previsto dagli artt. 2-*quater* e 139 del Codice (provv. 29 novembre 2018, n. 491, doc. web n. 9067692).

9 Cyberbullismo

Un ruolo a parte rivestono le segnalazioni presentate ai sensi della legge n. 71/2017 “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”.

Come già riportato nella Relazione per l’anno 2017 (p. 86), al fine adempiere al mandato conferito all’Autorità in questa materia, sul sito web istituzionale è stata creata una sezione dedicata (https://www.garanteprivacy.it/cyberbullismo), nella quale sono presenti un’infografica – recante un’informazione sintetica del contenuto della legge – e un modello di segnalazione da inviare attraverso una specifica casella di posta elettronica (cyberbullismo@gpdp.it).

A partire dall’entrata in vigore della legge citata, le istanze pervenute hanno riguardato in prevalenza la richiesta di rimozione di contenuti offensivi ai danni di minorenni, talvolta legati anche a immagini degli interessati, per la maggior parte riferite ai *social network* più noti, con i quali sono stati attivati specifici canali di comunicazione.

Un numero più limitato di segnalazioni ha riguardato il furto di identità e la creazione di falsi profili nell’ambito dei medesimi *social network*.

I casi segnalati sono stati definiti prevalentemente con la rimozione dei contenuti oggetto di doglianza. In alcuni casi particolari le questioni rappresentate hanno trovato adeguata definizione attraverso contatti interlocutori con i segnalanti, in occasione dei quali sono stati forniti chiarimenti operativi (quali il coinvolgimento del dirigente scolastico o del referente per il cyberbullismo nella scuola).

10 Marketing, profilazione e trattamento dei dati personali

10.1. *Verifiche preliminari*

Anteriormente al 25 maggio 2018, data a partire dalla quale ha trovato applicazione il RGPD, l'Autorità ha esaminato una pluralità di richieste di verifica preliminare presentate ai sensi dell'art. 17, d.lgs. n. 196/2003 da parte di società operanti nel settore della moda. Tali istanze, finalizzate al prolungamento dei tempi di conservazione dei dati della clientela in vista del loro trattamento per finalità di profilazione e marketing rispetto all'offerta di prodotti di fascia medio-alta per un arco temporale superiore a quello stabilito dal Garante nel provvedimento generale del 24 febbraio 2005 (doc. web n. 1103045), hanno formato oggetto di valutazione conformemente all'indirizzo seguito in passato dall'Autorità. In particolare, si è ritenuto che il settore merceologico di riferimento, che si caratterizza per la saltuarietà degli acquisti, consente un'analisi significativa delle informazioni acquisite ai fini delle menzionate finalità (sul presupposto della sussistenza di un consenso informato e distinto per ciascuna di esse da parte degli interessati) solo ove sia possibile per il titolare conservare e trattare i dati della propria clientela per un periodo di tempo più ampio rispetto a quello fissato, in termini generali, nel richiamato provvedimento del 2005. Si è quindi ritenuto congruo, come già in passato in casi analoghi, fissare in sette anni il tempo massimo di conservazione dei dati.

Con provvedimento 16 maggio 2018, n. 294 (doc. web n. 8998339), il Garante ha autorizzato un'azienda *leader* in Italia e nel mondo nel settore della moda e del lusso, che commercializza prodotti il cui acquisto si realizza in media una o due volte l'anno (rispetto ai quali è prevista una garanzia di 2 anni) e che, peraltro, offre ai clienti un servizio *post* vendita anche su capi che hanno un'anzianità superiore, a conservare i dati dei clienti e dei potenziali clienti per un periodo massimo di sette anni a decorrere dalla loro registrazione, ferma restando la loro automatica cancellazione o anonimizzazione irreversibile allo scadere del predetto termine. Con altri due provvedimenti del 18 aprile 2018, n. 233 (doc. web n. 8997404) e 9 maggio 2018, n. 274 (doc. web n. 8998319) il Garante ha esaminato le istanze, anch'esse formulate ai sensi del menzionato art. 17, provenienti da importanti società che progettano, producono e commercializzano autoveicoli e, sulla base di quanto dalle stesse rappresentato in ordine alla particolare tipologia di prodotti (la cui frequenza media di acquisto è pari a una/due volte in un decennio), ha individuato come proporzionato un arco temporale di dieci anni per la conservazione ed il trattamento ai fini di profilazione dei dati dei clienti e dei potenziali clienti, decorsi i quali i dati devono essere automaticamente cancellati o anonimizzati.

Con riguardo, invece, ad altri aspetti del trattamento, pure rappresentati nelle istanze ma non oggetto specifico delle stesse, si è ritenuto opportuno invitare gli istanti, considerata lo scenario normativo definito dal RGPD, di imminente applicazione, con particolare riferimento al principio di responsabilizzazione (artt. 5, par. 2, e 24 del RGPD), all'adozione di adeguate misure tecnico-organizzative volte a garantirne la conformità alle nuove disposizioni. È stato altresì evidenziato l'obbligo per il titolare, laddove il trattamento comporti un rischio elevato per i diritti e le libertà fondamentali delle persone, di effettuare, prima di procedere al tratta-

mento, una valutazione d'impatto sulla protezione dei relativi dati (art. 35, par. 1, del RGPD), peraltro doverosa ove ricorra una valutazione sistematica e globale di aspetti delle persone fisiche basate su trattamenti automatizzati come la profilazione, sulla scorta della quale vengano adottate decisioni con effetti giuridici o comunque significativi per gli interessati (art. 35, par. 3, lett. *a*), del RGPD; cfr. al riguardo i provv.ti 22 maggio 2018, n. 319, doc. web n. 9018611; n. 320, doc. web n. 9018628; n. 321, doc. web n. 9019882; n. 322, doc. web n. 9019890; n. 323, doc. web n. 9019902; n. 324, doc. web n. 9020242; n. 325, doc. web n. 9020250).

Al contrario, con riguardo ad analoghe istanze di verifica preliminare presentate da società operanti sia nel campo della moda che della cosmesi, il Garante ha ritenuto, in considerazione della tipologia e delle caratteristiche dei prodotti offerti (in quanto appartenenti ad una fascia di consumo medio-bassa e con una ricorrente frequenza di spesa), insussistenti i presupposti per riconoscere alle società un'estensione dei tempi di conservazione dei dati della propria clientela per periodi superiori a quelli indicati nel citato provvedimento generale del 24 febbraio 2005 (provv.ti 22 maggio 2018, n. 326, doc. web n. 9020258; n. 327, doc. web n. 9020270; n. 328, doc. web n. 9022048; n. 329, doc. web n. 9022056).

Il Garante ha altresì valutato una richiesta di verifica preliminare presentata da due società con riguardo all'offerta, rivolta alla clientela, di servizi di raccolta, analisi ed elaborazione di dati, asseritamene anonimi, attraverso l'utilizzo di un *device* dotato di videocamera, da installarsi sul soffitto dei locali o in prossimità delle vetrine dei negozi, per la rilevazione, ai fini di marketing e ricerche di mercato, delle immagini, dei comportamenti nonché dei dispositivi mobili con servizio wi-fi attivo, presenti nelle vicinanze del *device*, rilevandone il relativo *mac address* (quindi "crittografato in modo irreversibile"). Nonostante l'asserita elaborazione dei dati così rilevati in forma anonima (tale da non consentire la visione in diretta delle immagini raccolte) e l'assenza di una memorizzazione permanente delle immagini rilevate, il Garante ha rigettato l'istanza in ragione delle caratteristiche tecniche del dispositivo che comportavano l'acquisizione, seppure per un breve periodo, di dati personali (quali, oltre alle immagini relative agli interessati, anche il *mac address* dei dispositivi mobili utilizzati). D'altro canto, il descritto passaggio di persone ed oggetti attraverso linee virtuali tracciate nello spazio di ripresa si atteggiava come un vero e proprio tracciamento di mobilità (stante la possibilità di seguire, proprio grazie alle telecamere, la traiettoria individuale nell'area monitorata o i movimenti dei dispositivi mobili); ciò senza che fosse stato manifestato il necessario preventivo consenso informato degli interessati previsto dall'art. 122, d.lgs. n. 196/2003 (con riguardo all'accesso ad informazioni archiviate nell'apparecchio terminale di un contraente o di utente), la cui necessità è ribadita nell'*Opinion* del WP29 01/2017 *"on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)"*, ed in assenza di altro presupposto giuridico idoneo a legittimare il trattamento quale, in particolare, il legittimo interesse del titolare (provv. 22 maggio 2018, n. 360, doc. web n. 9022068).

10.2. *Telefonate indesiderate a contenuto promozionale*

Come già indicato in passato (cfr. Relazione 2016, p. 83 ss.; Relazione 2017, p. 88), le segnalazioni – alle quali nel 2018 si sono aggiunti anche numerosi reclami formulati ai sensi del Regolamento generale europeo in base al modello messo a disposizione dall'Autorità sul proprio sito istituzionale al fine di agevolare la loro

corretta formulazione – pervenute in materia di marketing hanno riguardato, in assoluta prevalenza, il cd. telemarketing selvaggio e, in misura residuale, comunicazioni commerciali via e-mail o sms.

A seguito dell'adozione (già segnalata nella precedente Relazione) della legge 11 gennaio 2018, n. 5, "Nuove disposizioni in materia di iscrizione e funzionamento del Registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato", preordinata a favorire un più efficace contrasto del telemarketing selvaggio, sono proseguiti i lavori per l'adozione del decreto del Presidente della Repubblica previsto dall'art. 1, comma 15 della medesima legge, finalizzato ad apportare le opportune modifiche alle disposizioni regolamentari vigenti che disciplinano le modalità di iscrizione e funzionamento del registro delle opposizioni nonché ad abrogare eventuali disposizioni regolamentari incompatibili con il nuovo quadro normativo; rispetto ad esso sono in corso presso l'Autorità le necessarie valutazioni per l'adozione del parere del Garante.

Con particolare riguardo all'ambito del telemarketing, migliaia permangono le segnalazioni portate all'attenzione del Garante che, in ragione della loro numerosità e della complessità delle operazioni necessarie per risalire all'effettiva (sovente articolata) "filiera" del trattamento (con la conseguente individuazione delle relative responsabilità), continuano a costituire il "carico" di lavoro assolutamente prevalente dell'Autorità (per un'analisi di dettaglio v. sez. IV, tab. 10). Specie con riguardo alle segnalazioni presentate nei confronti di taluni operatori, non si registrano purtroppo segnali tangibili di flessione malgrado gli interventi e i conseguenti provvedimenti di varia natura (inibitori, prescrittivi e sanzionatori) già adottati dall'Autorità (e puntualmente indicati nelle precedenti Relazioni).

Dall'analisi delle segnalazioni complessivamente pervenute risulta che le telefonate indesiderate continuano ad interessare sia gli abbonati iscritti nel Registro pubblico delle opposizioni (Rpo) – circostanza dalla quale si devono quindi desumere comportamenti tutt'altro che virtuosi da parte di non pochi soggetti operanti nella (non di rado lunga) filiera del telemarketing, che dal committente della campagna promozionale si snoda fino all'ultimo anello della stessa, l'operatore che materialmente effettua la chiamata – sia i titolari di numerazioni (residenziali e, sempre più spesso, mobili) non pubblicate su elenchi telefonici (cd. numerazioni riservate).

I settori merceologici nei quali operano i committenti oggetto di segnalazione continuano ad essere soprattutto quello telefonico ed energetico, con una differenziata consistenza numerica delle segnalazioni rispetto a ciascuno degli operatori. Modalità particolarmente aggressive (oltre che la mancata identificazione del committente) vengono segnalate rispetto a chiamate promozionali nel settore finanziario e valutario (aventi genericamente a contenuto "Forex" o "Trading").

Non di rado, come pure segnalato in passato, le telefonate promozionali indesiderate vengono eseguite da parte di *call center* stabiliti al di fuori del territorio nazionale, all'esito di processi di delocalizzazione delle attività economiche per le ragioni più varie, perlopiù di natura fiscale e giuslavoristica.

Continua a rilevarsi il fenomeno delle telefonate effettuate, in violazione di legge, con numerazione chiamante oscurata.

Sotto un diverso profilo, persistono i casi nei quali viene lamentato il mancato o tardivo riscontro con riguardo all'esercizio dei diritti degli interessati da parte degli operatori economici nel cui interesse si lamentano essere effettuate le comunicazioni promozionali – fenomeno già segnalato (cfr. Relazione 2017, p. 89; Relazione 2016,

p. 85; in merito, v. già provv. 21 settembre 2016, n. 368, doc. web n. 5774043; v. altresì provv.ti 22 giugno 2016, n. 275, doc. web n. 5255159, punti 7.2 e 7.3; 21 luglio 2016, n. 317, doc. web n. 5436585) e talora emerso anche nell'ambito di decisioni adottate su ricorso (v., ad es., provv.ti 16 marzo 2017, n. 149, doc. web n. 6503967; 6 aprile 2017, n. 184, doc. web n. 654439; 31 maggio 2017, n. 260, doc. web n. 6608298; 23 novembre 2017, n. 501, doc. web n. 7666773). In particolare, vengono lamentate, non solo la violazione del diritto di opposizione all'ulteriore trattamento per finalità di marketing, ma anche, in spregio dei diritti di accesso ai propri dati, l'assenza o la carenza di riscontro rispetto alle necessarie indicazioni, ad esempio, circa l'origine dei medesimi, elemento conoscitivo imprescindibile al fine di consentire all'interessato di risalire agli archivi che stanno a monte delle comunicazioni telefoniche ricevute.

Il riscontro ai segnalanti

In attuazione delle normativa regolante l'attività istituzionale del Garante (anche come riformulata dal decreto legislativo n. 101/2018 per l'adeguamento del Codice al RGPD), l'Autorità – che ha peraltro riformulato le FAQ presenti sul proprio sito web (v. doc. web n. 1794339) – ha continuato nel 2018, pur a fronte di risorse limitate rispetto alle molteplici e complesse funzioni assegnate dal legislatore, a dare riscontro individualizzato a larga parte delle (migliaia di) segnalazioni pervenute (sovente da parte di segnalanti che reiteratamente, o anche solo episodicamente, hanno lamentato la persistenza dei contatti indesiderati, nonostante l'esercizio del diritto di opposizione o l'iscrizione della propria numerazione nel Rpo). Ciò, anzitutto al fine di rendere edotti gli interessati della particolare attenzione dedicata dall'Autorità alla problematica del marketing indesiderato, oltre che della possibilità di considerare le loro doglianze, in forma comunque "aggregata", in vista dell'accertamento della correttezza e legittimità dei trattamenti posti in essere.

Nei medesimi riscontri, anche al fine di favorire la conoscenza della materia di protezione dei dati e dell'attività di controllo del Garante, vengo indicati i provvedimenti assunti e forniti alcuni suggerimenti pratici su come bloccare comunicazioni non gradite. Con analoghi riscontri, peraltro, sono state costantemente fornite informazioni corrette sugli strumenti messi a disposizione dall'ordinamento a vantaggio degli interessati per prevenire od opporsi alle telefonate indesiderate e/o per ricevere informazioni sull'origine dei propri dati nella disponibilità delle imprese committenti o incaricate dell'attività di telemarketing (o per esercitare gli altri diritti di cui all'art. 7, d.lgs. n. 196/2003, ribaditi e in parte innovati dagli artt. 15-22 del RGPD, anche avvalendosi del modello predisposto dall'Autorità: cfr. doc. web n. 1089924).

In questa prospettiva, nelle comunicazioni individuali si sono invitati i segnalanti a non escludere la possibilità, quantomeno in taluni casi, della liceità del contattato commerciale sulla base di un consenso prestato, anche per inavvertenza, a vantaggio del medesimo operatore economico nel cui interesse si è contattati (come, in occasione dell'acquisto di beni o servizi forniti) o a terzi (ad es., partecipando a concorsi a premi, o autorizzando tali usi su siti web di natura più varia per l'utilizzo, magari senza corrispettivo, di alcuni servizi), anche sulla base di un consenso, talora illegittimamente acquisito, come nei casi di cd. consenso obbligato (materia su cui il Garante ha continuato ad intervenire anche nel 2018: v. ad es., provv. 22 maggio 2018, n. 363, doc. web n. 8995274, di seguito sinteticamente illustrato).

Nella medesima prospettiva di attenzione alle doglianze dei segnalanti riguardo al telemarketing, fenomeno lesivo in vero non solo del diritto alla protezione dei dati ma anche di altri diritti fondamentali della persona, come quello alla tranquillità individuale, comunicazioni puntuali sono state regolarmente inviate anche con

Accertamenti telemarketing presso operatori telefonici

riferimento alle numerose e reiterate segnalazioni riguardanti telefonate promozionali provenienti da soggetti, od effettuate per conto di committenti, non individuati, o per le quali non è stata indicata la/e numerazione/i chiamante/i o altri elementi (come la data e l'ora dei contatti indesiderati) essenziali ai fini di un'attività – efficiente ed efficace – di controllo dell'Autorità.

L'attività di controllo in relazione al fenomeno del cd. telemarketing selvaggio è stata intensa anche nel 2018 e contrassegnata dall'adozione, all'esito dei provvedimenti di seguito sinteticamente descritti, di ordinanze ingiunzione per l'importo complessivo, limitatamente al settore in esame, di 3.440.000 euro (provv.ti 18 gennaio 2018, n. 16, doc. web n. 7665804; 22 maggio 2018, n. 330, doc. web n. 9018431, 5 luglio 2018, n. 412, doc. web n. 9025351; 26 luglio 2018, n. 441, doc. web n. 9040267; 29 novembre 2018, n. 493, doc. web n. 9079005) (cfr. par. 21.6.2).

Numerose richieste di informazioni – concernenti casi singoli individuati per tipologia e gravità della violazione ipotizzata, o anche in via cumulativa (ovvero istruendo congiuntamente più segnalazioni di contenuto analogo) – sono state rivolte alle società telefoniche, essendo tra le principali destinatarie di segnalazioni e reclami per l'effettuazione di telefonate e l'invio di sms promozionali indesiderati, talora anche in tempi successivi all'opposizione fatta valere reiteratamente dagli interessati. Ciò, al fine di acquisire elementi utili a verificare le misure organizzative nonché l'approccio complessivamente adottato da tali titolari per assicurare il corretto trattamento dei dati degli interessati e l'effettivo adempimento degli obblighi imposti dalla normativa, anche alla luce della piena operatività del RGPD. Sono altresì proseguiti gli accertamenti ispettivi, effettuati ai sensi degli artt. 157 e, talora, 158 del Codice, presso le sedi legali e operative di tali società e/o dei loro *dealer* incaricati dello svolgimento delle campagne promozionali, sulla base delle liste fornite dalle committenti o nella autonoma disponibilità degli stessi.

Grazie alle verifiche ispettive svolte e alla documentazione acquisita nell'ambito dell'istruttoria, in un caso il Garante ha potuto accertare che, nell'arco dei 18 mesi presi in considerazione dalle verifiche, sono state effettuate, nell'interesse di una società telefonica, fino a 2 milioni di telefonate promozionali e inviati circa 22 milioni di sms senza un valido consenso degli interessati. Le anomalie e i trattamenti illeciti rilevati hanno riguardato sia clienti attuali o ex clienti, sia quelli potenziali (cd. *prospect*). Le offerte commerciali indesiderate venivano rivolte ad utenti che non avevano fornito il consenso al trattamento dei propri dati personali per finalità di marketing, ma anche a coloro che avevano espressamente chiesto di non essere più disturbati o di veder cancellati i propri contatti dai *database* della società e dei *call center* da questa utilizzati per finalità promozionali. Nell'occasione è emerso che anche in caso di chiaro diniego ai contatti a contenuto promozionale – volontà di cui gli operatori tenevano traccia con la frase "non chiamare mai più" – la compagnia telefonica considerava la richiesta solo come una mera sospensione del consenso, procedendo a ricontattare l'utente in successive campagne promozionali. Sono stati rilevati vari profili di inidoneità anche rispetto alle informative fornite agli interessati. Alla luce dei vari illeciti rilevati e ritenuto violato il principio di correttezza previsto dal decreto legislativo n. 196/2003, il Garante ha vietato alla medesima società l'ulteriore trattamento per finalità di marketing dei dati personali trattati in assenza del consenso espresso degli utenti da contattare, prescrivendo l'adozione, senza ritardo, delle necessarie misure tecnico-organizzative volte a registrare tempestivamente e correttamente l'opposizione al trattamento nonché a prevenire i contatti commerciali indesiderati. Al medesimo titolare del trattamento è stato altresì prescritto di procedere a una veri-

fica puntuale delle modalità con cui acquisisce il consenso dagli interessati nei vari contesti in cui tale attività veniva realizzata (ad es., sia tramite la propria rete commerciale, piattaforme web, etc.) (provv. 8 marzo 2018, n. 140, doc. web n. 8233539).

All'esito degli accertamenti relativi ai contatti commerciali effettuati nell'interesse di altra società telefonica, nell'intervallo temporale compreso tra i mesi di gennaio 2016 e ottobre 2017 sono state riscontrate innumerevoli irregolarità, in particolare relative ad attività di marketing effettuate in assenza del consenso degli interessati. Il Garante ha anche rilevato un numero considerevole di telefonate verso numerazioni proposte autonomamente dai *partner* della medesima società – oltre 8 milioni di telefonate riferibili a 2,7 milioni di persone – e non inserite nelle cosiddette liste di contattabilità trasmesse dalla compagnia telefonica (cd. fuori lista). In questi casi la società non era in grado di garantire che le persone contattate non fossero iscritte al Registro delle opposizioni o non si fossero comunque opposte a contatti commerciali. Irregolarità sono state individuate anche nella cosiddetta procedura di "*call me back*" (richiamami) attivata sul sito web della società in questione: la richiesta di essere contattato mediante apposito pulsante *online* veniva infatti qualificata dalla società quale autorizzazione all'utilizzo dei propri dati personali per finalità di marketing e di profilazione, senza che l'utente fosse messo in condizione di manifestare una scelta realmente libera e specifica per le differenti finalità di trattamento. Il Garante ha inoltre rilevato che alcune forme di profilazione della clientela, come l'indicazione "persona anziana" (riferibile a un milione di individui) oppure "alto" o "basso spendente", erano definite sulla base di dati imprecisi e, comunque, in assenza del preventivo specifico consenso informato degli interessati. A seguito degli accertamenti in parola, la società ha provveduto autonomamente a modificare le procedure e ad aggiornare i propri sistemi nella prospettiva di risolvere le criticità riscontrate nel corso delle verifiche. Il Garante ha comunque vietato alla compagnia telefonica di trattare ulteriormente, per finalità di marketing, i dati di quanti non avessero manifestato un libero consenso o lo avessero revocato o comunque fatto valere il diritto di opposizione (provv. 18 aprile 2018, n. 235, doc. web n. 9358243). Nella medesima occasione il Garante ha anche vietato al titolare in questione di profilare gli utenti senza averli prima informati e aver acquisito, anche in questo caso, il loro consenso; è stato inoltre prescritto alla società di controllare la condotta dei propri *partner* commerciali e il corretto funzionamento della piattaforma informatica utilizzata, nonché di adottare misure tecniche e organizzative che assicurassero il tracciamento di tutte le telefonate promozionali.

Muovendo da numerose segnalazioni pervenute in merito a telefonate e sms promozionali asseritamente ricevuti nonostante l'espressa negazione del consenso, il Garante ha svolto un accertamento ispettivo nei confronti di altro primario operatore telefonico, effettuando verifiche anche presso i relativi *partner* commerciali. Da tali accertamenti è emerso che la società non aveva posto in essere adeguate misure tecnico-organizzative volte a registrare tempestivamente l'opposizione al trattamento per finalità promozionali, né aveva predisposto sufficienti controlli sull'attività svolta dai propri *partner* commerciali e non era stata in grado di identificare i soggetti che, nella filiera dei subappalti, avevano posto in essere l'attività promozionale nel proprio interesse. Nella maggior parte dei casi, peraltro, tali *partner* erano stati qualificati come titolari autonomi del trattamento pur avendo accesso diretto a tutti i dati contenuti nei sistemi della compagnia e senza margini di autonomia circa le finalità del trattamento. Alla luce di tali risultanze, il Garante ha vietato l'ulteriore trattamento per finalità di marketing dei dati acquisiti in assenza di un con-

Automotive

senso libero e informato ed ha prescritto all'operatore di adottare alcune misure tecnico-organizzative volte a tracciare le attività promozionali effettuate dai terzi e a tenere traccia dei dinieghi al trattamento espressi dagli interessati (provv. 22 maggio 2018, n. 313, doc. web n. 8995285).

Muovendo da una segnalazione avente ad oggetto telefonate indesiderate da parte di una società automobilistica e alla luce degli elementi istruttori complessivamente acquisiti, con riferimento anzitutto ai dati personali riferiti al segnalante, l'Autorità ha ritenuto violata, da parte della medesima, la disciplina di protezione dei dati personali, essendo stato l'interessato contattato in assenza di un valido consenso al trattamento dei propri dati personali per finalità di marketing. Infatti, è risultato confermato il contatto commerciale avvenuto nell'interesse della società in assenza del consenso dell'interessato, circostanza peraltro registrata nei sistemi della società, in violazione di quanto previsto dagli artt. 23 e 130, comma 3, d.lgs. n. 196/2003 (in tal senso già provv. 22 giugno 2016, n. 275, doc. web n. 5255159, oggetto di integrale conferma da parte di Trib. Milano, sez. I civ., 5 maggio 2017, n. 5022; provv. 15 giugno 2017, n. 268, doc. web n. 6629169; v. pure provv. 1° ottobre 2015, n. 503, doc. web n. 4449190). Più radicalmente, al di là della singola posizione, gli accertamenti svolti sulle campagne promozionali effettuate mediante il canale telefonico nell'interesse della società hanno consentito di appurare che la medesima, nel contattare utenze rispetto alle quali il consenso degli interessati non era stato manifestato o rispetto ai quali risultava la volontà a non essere contattati (con consenso valorizzato a "no" nei sistemi), ha operato in violazione della disciplina di protezione dei dati personali (v. artt. 23 e 130, d.lgs. n. 196/2003). Sulla base della documentazione trasmessa dalla società riferita alle campagne di telemarketing svolte nel periodo gennaio-dicembre 2017, è stata verificata l'esistenza nelle cd. liste di contattabilità formate dalla società di numerazioni che non avrebbero dovuto essere contattate stante l'assenza di un valido consenso da parte degli interessati. Sono così risultati illecitamente oggetto di contatto commerciale: oltre 3.900 interessati il cui consenso al trattamento per finalità di marketing era valorizzato a "no" o non espresso; rispetto ad ulteriori 11.300 interessati il consenso alla comunicazione dei dati per finalità di marketing era parimenti valorizzato a "no" o non espresso. Anche rispetto a tali verifiche, l'Autorità ha adottato un provvedimento di divieto dell'ulteriore trattamento dei menzionati dati personali per finalità pubblicitarie (provv. 18 aprile 2018, n. 236, doc. web n. 8983292).

Compravendita di liste e telemarketing

Al fine di contrastare il fenomeno del telemarketing indesiderato è stata posta particolare attenzione anche all'utilizzo di banche dati acquisite da terzi per finalità promozionali; tale fattispecie può presentare infatti criticità, in particolare quando la raccolta dei dati direttamente degli interessati da parte dei soggetti cedenti, o da parte dei loro danti causa, talora ubicati all'estero, avviene in violazione dei principi di correttezza, liceità e finalità oppure in assenza del consenso degli interessati, informato e specifico rispetto al trattamento per finalità promozionali (artt. 23 e 130, d.lgs. n. 196/2003).

All'esito di accertamento ispettivo condotto nei confronti di un *call center* operante in subappalto per conto di operatori telefonici, il Garante ha dichiarato illecito, e conseguentemente ha vietato, il trattamento posto in essere utilizzando una banca dati contenente oltre 400.000 numerazioni telefoniche, acquisita da un soggetto anonimo contattato tramite Facebook in assenza di un consenso specifico e informato degli interessati (provv. 15 febbraio 2018, n. 79, doc. web n. 7980857; per analogo accertamento e per i principi ribaditi dal Garante in tali fattispecie v. provv. 22 maggio 2018, n. 363, doc. web n. 8995274; v. al riguardo le ordinanze

ingiunzione adottate con provv.ti 31 maggio 2018, n. 368, doc. web n. 9038227; n. 369, doc. web n. 9038386).

10.3. *Invio di comunicazioni a contenuto promozionale agli indirizzi Pec dei liberi professionisti*

Il Garante ha vietato a una società e a un'associazione ad essa collegata l'invio di e-mail promozionali indesiderate a liberi professionisti, utilizzandone gli indirizzi di posta elettronica certificata (provv. 1° febbraio 2018, n. 52, doc. web n. 7810723). Dalle verifiche – avviate a seguito di numerose segnalazioni ed effettuate con l'ausilio del Nucleo speciale *privacy* della Guardia di finanza – è emerso che alcuni collaboratori volontari dell'associazione e una società terza avevano reperito *online*, massivamente, gli indirizzi Pec di avvocati e, in minor parte, di altri liberi professionisti (commercialisti, revisori contabili, consulenti del lavoro, notai), con varie modalità, manuali e automatizzate. La società aveva poi spedito comunicazioni a contenuto promozionale (relative alla notizia della pubblicazione di un bando di selezione per "consulente reputazionale", l'invito a partecipare ad un *webinar* ed articoli concernenti la società mittente) utilizzando tali recapiti, in numero complessivo superiore alle 800.000 e-mail. Oltre ad essere stati trattati senza il necessario consenso, gli indirizzi pec sono risultati rastrellati massivamente (cd. *web scraping*) mediante appositi *software* da varie fonti presenti sul web: il registro Ini-Pec (ridenominato "Indice nazionale dei domicili digitali" a seguito del decreto legislativo n. 217/2017); il sito www.registroimprese.it; gli elenchi pubblicati da alcuni ordini professionali provinciali.

Tale condotta è stata ritenuta in contrasto con la normativa di settore, e in particolare con: l'art. 6-*bis*, comma 1, d.lgs. n. 82/2005 (Codice dell'amministrazione digitale - Cad, introdotto dall'art. 5, comma 3, d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla l. 17 dicembre 2012, n. 22), secondo il quale la finalità di tali indirizzi consiste nel "favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica"; l'art. 16, comma 10, d.l. n. 185/2008 (convertito, con modificazioni, in legge 28 gennaio 2009, n. 2), in base al quale l'estrazione di elenchi di indirizzi di posta elettronica certificata contenuti nel registro delle imprese o negli albi o elenchi "è consentita alle sole pubbliche amministrazioni per le comunicazioni relative agli adempimenti amministrativi di loro competenza".

L'Autorità ha inoltre chiarito che, rispetto all'invio delle comunicazioni elettroniche in questione, considerato il loro contenuto promozionale, l'associazione e la società, in qualità di co-titolari del trattamento, avrebbero dovuto acquisire il consenso informato degli interessati ai sensi degli artt. 13, commi 1 e 4, 130, commi 1 e 2, e 23, d.lgs. n. 196/2003 (v. pure Linee guida in materia di spam, 4 luglio 2013, doc. web n. 2542348, in particolare punto 2.6). Peraltro, il Garante ha ribadito che la necessità del previo consenso informato dell'interessato sussiste anche quando i dati personali (come, nella fattispecie, una parte degli indirizzi di posta elettronica destinatari delle comunicazioni in parola) siano rinvenibili in altri registri o elenchi pubblici (quali quelli disponibili sul sito www.registroimprese.it o sui siti web istituzionali degli ordini provinciali delle categorie professionali), in quanto l'agevole reperibilità degli stessi non ne autorizza il trattamento per qualsiasi scopo, ma soltanto per le specifiche finalità sottese alla loro pubblicazione (principio costantemente affermato dal Garante a partire dal provv. 11 gennaio 2001, doc. web n.

40823 e, quindi, con il provv. generale sullo *spamming*, 29 maggio 2003, doc. web n. 29840 e con le Linee guida spam, punto 2.5; v. altresì provv. 6 ottobre 2016, n. 390, doc. web n. 5834805; provv. 21 settembre n. 2017, n. 378, doc. web n. 7221917; provv. 30 novembre 2017, n. 503, doc. web n. 7522090).

Né, si è ribadito, viene meno l'illiceità del trattamento in ragione dell'inserimento nelle e-mail indesiderate di un *link* per la cancellazione dalla *mailing list*, poiché il consenso richiesto (salvo per le ipotesi di cui all'art. 130, comma 4, d.lgs. n. 196/2003, cd. *soft spam*) deve essere legittimamente acquisito anteriormente all'invio delle comunicazioni promozionali (cfr., fra i vari, Linee guida 4 luglio 2013, punto 2.5; provv.ti 6 ottobre 2016 e 30 novembre 2017, cit.).

Nell'occasione, non sono state ritenute valide le argomentazioni addotte a sostegno della correttezza del proprio operato dalla società e dall'associazione, le quali, tra l'altro, si ritenevano esentate dalla richiesta del consenso preventivo sulla base della presunta natura "istituzionale" delle comunicazioni (e in particolare, su riconoscimenti e patrocini ricevuti da parte degli Ordini professionali di appartenenza degli interessati), non potendo ritenersi tali circostanze idonee a surrogare il necessario consenso informato da parte dei singoli interessati, cui fa capo il diritto alla protezione dei dati personali riconosciuto dal legislatore. Le e-mail infatti, come ha chiarito il Garante, avevano in realtà carattere promozionale, in quanto miravano a favorire le attività dell'associazione connesse alla figura di "consulente reputazionale", e quindi dovevano essere inviate nel rispetto delle regole previste dal decreto legislativo n. 196/2003 e dalle citate Linee guida in materia di attività promozionale.

L'Autorità ha vietato, di conseguenza, alla società e all'associazione l'ulteriore illecito trattamento dei dati dei professionisti e ne ha prescritto, in ragione dell'origine illecita, la cancellazione, riservandosi di valutare i correlati profili sanzionatori.

10.4. *Utilizzo di* pop-up *con il consenso obbligato al trattamento per finalità di marketing*

Il Garante ha vietato a una società che offre servizi di comparazione sul proprio sito web (mutui, assicurazioni, luce, gas, telefonia) il trattamento, per finalità di marketing e di vendita ad altre aziende, dei dati raccolti attraverso un *pop up* senza il necessario consenso degli utenti (provv. 22 maggio 2018, n. 363, doc. web n. 8995274). L'intervento del Garante ha fatto seguito ad alcune segnalazioni riguardanti, a seconda dei casi, comunicazioni promozionali indesiderate ricevute dalla stessa società per telefono o per e-mail, oppure telefonate promozionali indesiderate, su utenze fisse e mobili, effettuate per conto di società dei settori energetico e delle telecomunicazioni.

Le verifiche ispettive hanno consentito di accertare che il *pop up* in questione non permetteva l'accesso ai servizi offerti se l'utente non accettava, con un consenso unico e obbligato, il trattamento dei dati per diverse finalità (fra le quali il marketing o la comunicazione dei dati a terzi).

In caso di compilazione delle caselle di testo, ma di mancata spunta del consenso, infatti, il sito non acquisiva i dati inseriti e non consentiva di procedere con la richiesta. Pertanto, ancorché l'informativa facesse riferimento alle diverse finalità di trattamento di dati, non si consentiva agli utenti di effettuare, come prevede la normativa, una scelta specifica e differenziata per ciascuna diversa finalità di trattamento.

Nel disporre il divieto, il Garante ha ribadito che la "raccolta" (al pari della conservazione) dei dati personali è in sé – a prescindere da eventuali ulteriori tratta-

menti – un'operazione di trattamento rilevante ai fini della normativa in materia e quindi protetta dalla medesima (v. art. 4, comma 1, lett. *a*), d.lgs. n. 196/2003; in questo senso, v., fra agli altri, i provv.ti 27 ottobre 2016, n. 439, doc. web n. 5687770; 20 novembre 2014, n. 532, doc. web n. 3657934), le menzionate violazioni sono da ritenersi assorbenti rispetto all'ulteriore violazione ravvisabile, in capo alla società, nella mancata acquisizione, al momento della raccolta, di un libero e specifico consenso degli utenti per l'invio di comunicazioni automatizzate a contenuto promozionale ai sensi dell'art. 130, commi 1 e 2, d.lgs. n. 196/2003.

L'Autorità ha ribadito che tali necessari requisiti del consenso sono chiaramente evidenziati anche dalle Linee guida in materia di attività promozionale e contrasto allo spam del 4 luglio 2013, e sono stati altresì sostanzialmente ribaditi dal RGPD (v., in particolare: artt. 6 e 7 e i considerando 42 e 43).

Nell'ottica di garantire la miglior conformità dei trattamenti di dati svolti, è stata inoltre prescritta alla società, qualora intendesse utilizzare in futuro il *pop-up* per raccogliere i dati a scopo promozionale (o per altre finalità), la riformulazione del *form* di raccolta dei dati mediante il menzionato *pop-up* affinché venga acquisito dagli utenti un consenso, oltre che informato e documentato per iscritto, anche libero, specifico e chiaramente formulato con riferimento alle finalità promozionali e alla prevista comunicazione a terzi.

È altresì emerso che nel medesimo *database* confluivano, in aggiunta ai dati raccolti sul citato sito web, anche i dati personali acquisiti da terzi (fra i quali alcuni segnalanti e alcuni soggetti selezionati a campione fra le liste di dati comunicate alla società dai propri fornitori di liste) rispetto ai quali né in sede di accertamento *in loco*, né successivamente sono stati forniti elementi idonei a comprovare l'avvenuta manifestazione del necessario consenso secondo le modalità previste dalla legge.

Pertanto, anche in relazione alle siffatte attività di marketing e di comunicazione a terzi, sono risultate violate le disposizioni di protezione dei dati personali (artt. 11, comma 1, lett. *a*) e *b*); 23, commi 1 e 3; 130, commi 1 e 2, d.lgs. n. 196/2003). Peraltro si evidenzia come l'obbligo di acquisizione del preventivo specifico consenso per le finalità promozionali (e, s'intende, per le altre diverse finalità non meramente endo-contrattuali od amministrative) sia stato ribadito dal Garante in più provvedimenti, generali e specifici (ad es., cfr. provv. 27 ottobre 2016, cit., e, fra gli altri, anche provv.ti 24 febbraio 2005, punto 7, doc. web n. 1103045; 20 dicembre 2012, doc. web n. 2223607; 1° ottobre 2015, n. 508, doc. web n. 4452896; 10 marzo 2016, n. 110, doc. web n. 4988238; 11 febbraio 2016, n. 49, doc. web n. 4885578; nonché, in termini più generali, anche nell'ambito delle citate Linee guida del 4 luglio 2013).

Il Garante ha pure ribadito che l'acquirente di banche dati deve verificare che "ciascun interessato abbia validamente acconsentito alla comunicazione del proprio indirizzo di posta elettronica ed al suo successivo utilizzo ai fini di invio di materiale pubblicitario" (cfr. già provv. generale 29 maggio 2003, par. 5).

Nella medesima circostanza, l'Autorità – in una prospettiva sistematica e integrata dei processi di trattamento e degli adempimenti in materia – ha ritenuto rilevante il possibile impatto di tali attività di trattamento sul fondamentale diritto alla protezione dei dati, nonché sul connesso diritto alla tranquillità individuale degli interessati (soprattutto, in considerazione del diffuso fenomeno del telemarketing indesiderato). Ciò, in ragione sia della mole dei dati personali trattati dalla società, sia del rischio concreto che il vizio originario del consenso di una parte delle liste acquisite dalla società da terzi si riverberi, in termini di illiceità, su ogni successiva attività di trattamento dei medesimi dati (quali l'eventuale invio di comunicazioni promozionali e/o l'eventuale ulteriore comunicazione/cessione a altri terzi per fina-

lità promozionali) effettuata da parte dei soggetti (cessionari), ai quali la società li abbia comunicati o ceduti (per le loro finalità promozionali).

Il Garante ha pertanto vietato anche il trattamento dei dati tratti da elenchi acquisiti da altre imprese e per i quali la società non sia stata in grado di comprovare la manifestazione del consenso libero e specifico degli interessati per finalità di marketing, né quello per la comunicazione ad altri soggetti per scopi promozionali. Inoltre, ha ordinato alla stessa di avvisare tutti i soggetti ai quali ha ceduto liste di dati personali che questi non possono essere utilizzati senza aver acquisito il necessario consenso per le proprie attività.

Per le violazioni riscontrate sono state contestate le corrispondenti sanzioni ammnistrative che la società ha provveduto ad oblare; per contrastare la circolazione di dati "viziati" ed ulteriori possibili trattamenti illeciti, come il telemarketing indesiderato, l'Autorità si è riservata di effettuare accertamenti anche nei confronti dei *partner* commerciali (provv.ti 26 luglio 2018, n. 442, doc. web n. 9052099; n. 443, doc. web n. 9054309).

11 Internet e servizi di comunicazione elettronica

11.1. *Scambio di dati fra Facebook e WhatsApp*

Il Garante ha chiuso l'istruttoria nei confronti di WhatsApp e Facebook avviata per violazioni della disciplina di protezione dei dati personali, adottando un provvedimento di divieto nei confronti dei due soggetti (provv. 4 ottobre 2018, n. 462, doc. web n. 9058572). L'istruttoria, iniziata nel settembre del 2016, è stata sospesa durante i lavori di un'apposita *task force*, composta dai rappresentanti delle diverse autorità di protezione dati europee e coordinata da quella britannica, che si sono conclusi a giugno 2018.

Il Garante ha accertato che WhatsApp aveva, di fatto, indotto i propri utenti ad accettare integralmente i nuovi "Termini di utilizzo", in particolare la condivisione dei propri dati con Facebook, acquisendo il consenso alla loro comunicazione per prodotti e inserzioni pubblicitarie in modo non conforme agli artt. 13 e 23, d.lgs. 196/2003, in quanto l'informativa è risultata essere stata resa in forma parziale ed inidonea ad illustrare compiutamente le finalità della condivisione dei dati fra le due società di tal che il consenso prestato è risultato non consapevolmente e liberamente espresso oltre che non validamente manifestato atteso che la manifestato sulla casella di spunta era già "flaggata".

Per tali motivi, ai sensi dell'art. 58, par. 2, lett. *f*), del RGPD, il Garante ha vietato a WhatsApp di comunicare a Facebook i dati dei propri utenti, il cui consenso fosse stato ottenuto con le modalità sopra indicate, e a Facebook di effettuarne comunque ogni ulteriore trattamento.

L'Autorità ha osservato inoltre che nella comunicazione dei dati tra le due piattaforme, effettuata per le finalità "*Business Analysis Analytics*" e "*Safety and Security*", il requisito del legittimo interesse, invocato come base giuridica dal titolare del trattamento, non risultava configurabile. Infatti, oltre non essere stata attivata la procedura di bilanciamento degli interessi coinvolti a cura del Garante ai sensi dell'art. 24, comma 1, lett. *g*), d.lgs. n. 196/2003, non sono stati comunque forniti idonei elementi di valutazione per poter verificare, ad esempio, se il trattamento perseguisse effettivamente il legittimo interesse dichiarato (tra gli altri, la sicurezza), se fosse necessario per la sua realizzazione, ossia contribuisse alla realizzazione di tale interesse meglio di altre possibili soluzioni meno invasive, in termini cioè tali da risultare superiore allo svantaggio arrecato agli interessati (sul punto cfr. il parere del WP29, 19 aprile 2014, n. 6/2014).

12 Il trattamento dei dati personali da parte di movimenti politici e associazioni

12.1. *Attività politica e piattaforme informatiche*

Anche nel corso del 2018 il Garante ha avuto occasione di interessarsi ai trattamenti di dati personali posti in essere da associazioni e partiti politici.

È infatti proseguita l'attività, avviata nel 2017 nei confronti dell'Associazione Movimento 5 Stelle a seguito di un *data breach* che ha interessato un elevato numero di iscritti alla piattaforma informatica dello stesso, volta ad accertare l'effettivo adempimento delle misure impartite dal Garante con provvedimento 21 dicembre 2017, n. 548 (doc. web n. 7400401) al fine di garantire che i trattamenti dei dati personali degli utenti dei diversi siti web riferiti al Movimento 5 Stelle siano conformi ai princìpi in materia di protezione dei dati personali.

In particolare, con provvedimento 16 maggio 2018, n. 289 (doc. web n. 8999795) il Garante, effettuate le opportune verifiche tecniche in ordine alle misure nel frattempo già adottate, da un lato ha rilevato alcuni profili di criticità rispetto ai quali ha fissato l'ulteriore termine del 30 giugno 2018 per la presentazione dei necessari approfondimenti e di documentazione aggiuntiva; dall'altro, con specifico riferimento alla prescrizione di cui al punto *e*), par. 7, del citato provvedimento 21 dicembre 2017, nell'accogliere la richiesta di proroga formulata dall'Associazione Rousseau (responsabile del trattamento) in ragione del rallentamento che l'attività di affidamento in *outsourcing* del servizio di *auditing* informatico avrebbe subìto, anche a causa degli impegni connessi al periodo di campagna elettorale, ha fissato al 30 settembre 2018 il termine conclusivo per il completo adempimento di tutte le prescrizioni a suo tempo fornite.

Successivamente, con provvedimento 4 ottobre 2018, n. 461 (doc. web n. 9048594), avendo l'Autorità constatato – sulla base della documentazione trasmessa (le risultanze dei *security assessment)* – la sussistenza di debolezze strutturali degli applicativi testati e la conseguente necessità di adeguate contromisure nonché l'opportunità di concedere un periodo supplementare per l'adempimento di tutte le prescrizioni di cui al citato provvedimento del 21 dicembre 2017, anche alla luce della relazione tecnica presentata della società incaricata di realizzare le attività necessarie ad ottemperare alle prescrizioni anzidette, ha fissato al 15 ottobre 2018 il termine per il completo adempimento del provvedimento in questione. Sono seguiti nel mese di novembre accertamenti ispettivi *in loco*, comprensivi di analisi tecniche ed accessi a sistemi informatici, all'esito dei quali, con provvedimento 4 aprile 2019, n. 83 (doc. web n. 9101974), il Garante, alla luce del verificato non completo adempimento delle menzionate prescrizioni, ha assegnato ulteriori termini per dare attuazione allo stesso e per assicurare un quadro più adeguato di misure di sicurezza, specie con riferimento alle funzionalità di *e-voting*. Al contempo, con il medesimo provvedimento, il Garante ha sanzionato l'Associazione Rousseau relativamente ai profili di illiceità accertati.

Nel febbraio 2018 l'Autorità ha avviato un'istruttoria nei confronti del Partito democratico – Coordinamento cittadino di Firenze a seguito di una intrusione nei propri sistemi informatici, con conseguente violazione dei dati personali di circa 600 iscritti. Con provvedimento 10 gennaio 2019, n. 3 (doc. web n. 9082416) il

Garante, nel valutare le misure di sicurezza adottate e, in particolare, il ruolo svolto dalla società della cui infrastruttura il Pd Firenze si era avvalso, ha rilevato che la stessa avrebbe dovuto essere designata quale responsabile del trattamento e che tale mancata designazione ha configurato l'illiceità del trattamento in ragione dell'avvenuta comunicazione dei dati personali degli iscritti al partito a un soggetto terzo, in mancanza del consenso degli interessati.

Sono state definite altresì ulteriori istruttorie attivate nei confronti del Pd nazionale e del Pd Roma a seguito di segnalazioni individuali nelle quali si lamentava, tra l'altro, il persistente invio di sms a contenuto propagandistico anche in tempi successivi all'esercizio del diritto di opposizione da parte degli interessati. Alla luce degli elementi acquisiti, anche sulla scorta di precedenti decisioni del Garante – cfr. provv. gen. 6 marzo 2014, n. 107, doc. web n. 3013267, secondo il quale "con particolare riferimento al trattamento dei dati effettuato a fini di propaganda elettorale e comunicazione politica, l'interessato può in ogni momento opporsi alla ricezione di tale materiale, anche nel caso in cui abbia manifestato in precedenza un consenso informato. In tale ipotesi, il titolare è tenuto a non inviare più all'interessato ulteriori messaggi, anche in occasione di successive campagne elettorali o referendarie" – si è ritenuto che le comunicazioni in questione fossero state effettuate in violazione del principio di correttezza nel trattamento (art. 11, comma 1, lett. *a*), d.lgs. n. 196/2003) nonché del diritto di opposizione di cui all'art. 7, comma 4, lett. *a*), d.lgs. n. 196/2003 (cfr. note 25 gennaio 2018).

In altra fattispecie, rispetto all'uso per finalità propagandistiche dell'indirizzo di posta elettronica di una segnalante, risultato a seguito dell'istruttoria svolta acquisito da una candidata alle elezioni amministrative nell'ambito dell'esercizio delle funzioni istituzionali precedentemente svolte nel medesimo comune in qualità di assessore, si è ritenuto tale trattamento – in conformità a precedenti determinazioni adottate dal Garante (cfr. provv.ti 6 marzo 2014, n. 107, cit.; provv. 5 maggio 2016, n. 205, doc. web n. 6358149; già provv. 12 febbraio 2004, doc. web n. 634369) effettuato in violazione dei principi di correttezza e finalità (art. 11, comma 1, lett. *a*) e *b*), d.lgs. n. 196/2003), oltre che in assenza del necessario consenso dell'interessata (nota 25 gennaio 2018).

12.2. *Sms solidali*

Di diversa natura, ma sempre appartenente all'ambito associativo, è il riscontro fornito dall'Autorità ad un quesito, proposto da diversi enti del terzo settore, concernente la possibilità di "conoscere" i nominativi e i numeri di telefono dei donatori aderenti alle campagne di raccolta fondi effettuate via sms (cd. sms solidali) o mediante chiamata da rete fissa; ciò al fine di rendicontare il donatore circa gli esiti della campagna di raccolta fondi cui abbia aderito e, al contempo, renderlo edotto di nuove eventuali iniziative benefiche promosse dall'associazione. In merito l'Autorità, nell'esprimersi a favore della conoscibilità di tali informazioni, ha tenuto conto sia delle modifiche apportate dall'Agcom al Piano di numerazione nazionale in materia di servizi di raccolta fondi per fini benefici di utilità sociale (v. delibera Agcom n. 17/17/CIR), sia della recente riforma degli enti del terzo settore (legge n. 106/2016; decreto legislativo n. 117/2017), rinvenendo un particolare atteggiamento di favore del legislatore in materia di rendicontazione economica e sociale di tali enti del terzo settore, quale strumento volto a garantire la più ampia trasparenza e conoscibilità delle attività effettuate dagli stessi, nonché a comprovare un uso efficace ed efficiente delle elargizioni ricevute. In tale contesto, l'Autorità ha precisato

che l'attività di ricontatto del donatore per finalità di promozione di nuove iniziative benefiche è lecita solo a condizione di aver acquisito il preventivo consenso espresso dei donatori; consenso che può anche essere raccolto con modalità semplificate (tramite sms o mediante digitazione di un tasto). Sono state infine fornite specifiche prescrizioni in merito all'informativa (che, già nella forma sintetica, dovrà specificare le finalità e le relative basi giuridiche del trattamento), alla necessità che il titolare implementi un sistema che agevoli l'esercizio dei diritti dell'interessato (con particolare riferimento all'esercizio del diritto di revoca del consenso prestato, il quale deve poter essere esercitato "con la stessa facilità con cui è stato accordato"), nonché sull'individuazione dei tempi di conservazione dei dati dei donatori (che dovrebbero essere adeguati anche alla "natura" dell'iniziativa benefica da rendicontare nonché alla "risposta" in termini di fidelizzazione che di volta in volta sia fornita dall'interessato) (nota 24 ottobre 2018, doc. web n. 9058954).

13 La protezione dei dati personali nel rapporto di lavoro pubblico e privato

13.1. *Il rapporto di lavoro, pubblico e privato, e le prescrizioni già contenute nella autorizzazione generale n. 1/2016*

Il rapporto di lavoro, sia pubblico che privato, resta una delle principali aree di intervento del Garante. Salvo individuare nei diversi ambiti (pubblico e privato) gli interventi dell'Autorità nel corso del 2018, merita in anteparte evidenziare, con riferimento al trattamento dei dati sensibili, il citato provvedimento 13 dicembre 2018, n. 497 (doc. web n. 9068972), come detto posto in consultazione pubblica, con il quale il Garante ha inteso individuare, in conformità a quanto previsto dall'art. 21, d.lgs. n. 101/2018, le prescrizioni contenute (tra l'altro) nella autorizzazione generale n. 1/2016 in materia di lavoro che si ritengono compatibili con il RGPD e con il decreto legislativo n. 101/2018 di adeguamento del Codice.

Il provvedimento individua prescrizioni che produrranno effetti sino all'adozione delle regole deontologiche (cfr. artt. 2-*quater*, 21, comma 4, e 111, d.lgs. n. 101/2018) e la cui osservanza costituisce specifica condizione di liceità del trattamento (art. 21, comma 5, d.lgs. n. 101/2018).

Alla luce del quadro normativo delineato dal RGPD (e diversamente dall'impianto del decreto legislativo n. 196/2003 anteriormente alle modifiche del decreto legislativo n. 101/2018), i trattamenti dei dati personali nel contesto lavorativo, sono considerati sia se effettuati da datori di lavoro pubblici che privati (cfr. art. 88 e 9, par. 2, lett. *b*), del RGPD); pertanto le prescrizioni individuate nel provvedimento trovano applicazione nei confronti di tutti coloro, soggetti pubblici o privati, che in qualità di titolari autonomi (ad es., agenzie per il lavoro, datori di lavoro, medici competenti ai sensi della disciplina sulla sicurezza sul lavoro) o di responsabili del trattamento (ad es., consulenti del lavoro: cfr. al riguardo anche la risposta al quesito formulato dal Consiglio nazionale consulenti del lavoro, doc. web n. 9080970), effettuano trattamenti per finalità d'instaurazione, gestione ed estinzione del rapporto di lavoro.

Con il menzionato provvedimento sono state stabilite prescrizioni relative ai trattamenti dei dati che attengono sia alla fase preassuntiva, prodromica all'eventuale stipulazione del contratto di lavoro (e che, ad es., concernono i candidati ad un determinato impiego), sia allo svolgimento del rapporto (che si riferiscono ai lavoratori subordinati, o in rapporto di parasubordinazione, a soggetti che svolgono collaborazioni organizzate dal committente, o altri lavoratori autonomi in rapporto di collaborazione o ai titolari di cariche sociali, nonché ai familiari degli stessi, quando sia necessario trattare i relativi dati per la concessione di benefici di legge in favore del lavoratore).

Le prescrizioni individuate hanno ad oggetto il trattamento di specifiche tipologie di dati che, per la loro delicatezza, possono dar luogo nel contesto lavorativo ad un maggior rischio di discriminazione. Tra questi, ad esempio, i dati che rivelano le convinzioni religiose potranno essere trattati esclusivamente in caso di fruizione di permessi in occasione di festività religiose o per individuare le corrette modalità di erogazione dei servizi di mensa o, nei casi previsti dalla legge, per l'esercizio dell'obiezione di coscienza; con riguardo, invece, ai dati che rivelino le opi-

nioni politiche, è stato prescritto che, in caso di partecipazione ad operazioni elettorali in qualità di rappresentanti di lista, non debba essere richiesto, per il riconoscimento dei relativi giorni di assenza dal servizio, il documento che designa il rappresentate di lista essendo allo scopo sufficiente la certificazione del presidente di seggio.

Un altro gruppo di prescrizioni attiene alle modalità del trattamento dei dati, specificando i limiti che incontra il datore di lavoro quando procede alla trasmissione di atti mediante comunicazioni elettroniche individualizzate o in forma cartacea. In tale ambito, a titolo esemplificativo, una specifica prescrizione attiene ai trattamenti svolti per ragioni di organizzazione del lavoro (ad es., predisposizione dei turni di lavoro) in base alla quale non è giustificata l'indicazione, nemmeno attraverso acronimi o sigle, delle causali dell'assenza dalle quali sia possibile evincere particolari categorie di dati personali (ad es., permessi sindacali o dati sanitari).

Con il provvedimento in esame sono comunque fatte salve le disposizioni nazionali "più specifiche per assicurare la protezione dei diritti e delle libertà" dei lavoratori (art. 88 del RGPD) che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare, l'art. 113 del Codice, che fa salvo l'art. 8, l. n. 300/1970, e l'art. 10, d.lgs. 10 settembre 2003, n. 276, e che vietano, ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo.

13.2. *La protezione di dati nell'ambito del rapporto di lavoro privato tra vecchia e nuova disciplina*

Anche con riferimento ai trattamenti di dati personali effettuati nell'ambito del rapporto di lavoro il Garante ha tenuto conto della definitiva applicazione nel nostro ordinamento del RGPD a partire dal 25 maggio 2018. Sotto il profilo dei criteri di legittimazione dei trattamenti non si registrano modifiche significative. Per i trattamenti di dati "comuni" riferiti al lavoratore, il datore di lavoro continua ad effettuare – di regola – quelli necessari per l'esecuzione del contratto di lavoro e per adempiere agli obblighi derivanti dalle discipline lavoristiche di settore (v. art. 6, par. 1, lett. *b*) e *c*), del RGPD). Per quanto riguarda, invece, i dati sensibili, denominati "categorie particolari" di dati personali dal RGPD, quest'ultimo ha stabilito, in termini generali, che i relativi trattamenti che non siano fondati su uno dei presupposti indicati dall'art. 9, par. 2, del RGPD sono vietati. I trattamenti di dati sensibili effettuati per finalità di gestione del rapporto di lavoro (anche successivamente all'interruzione dello stesso) o in fase preassuntiva, possono essere effettuati solo in quanto necessari per l'adempimento di obblighi previsti da leggi e regolamenti oppure da un contratto collettivo nei limiti previsti dall'ordinamento (v. art. 9, par. 2, lett. *b*), del RGPD; v. pure, considerando n. 41). In ogni caso, il datore di lavoro tratta i dati dei propri dipendenti nel rispetto delle disposizioni nazionali "più specifiche per assicurare la protezione dei diritti e delle libertà" dei lavoratori (art. 88 del RGPD). Come anticipato, con particolare riferimento al trattamento dei dati sensibili l'Autorità, con provvedimento 13 dicembre 2018, n. 497 (posto in consultazione pubblica), ha individuato le prescrizioni contenute (tra l'altro) nella Autorizzazione generale n. 1/2016 in materia di lavoro che risultano compatibili con il RGPD e con il decreto legislativo n. 101/2018 di adeguamento del decreto legislativo n. 196/2003.

13

Dalla verifica preliminare alla valutazione di impatto *privacy*

Differentemente dal regime previgente i trattamenti dei dati personali nel contesto lavorativo, alla luce del quadro normativo delineato dal RGPD, sono quindi unitariamente disciplinati sia se effettuati da datori di lavoro pubblici che privati (cfr. art. 88 e 9, par. 2, lett. *b*), del RGPD).

Come anticipato (par. 1.3), a partire dal 25 maggio 2018 è stato soppresso l'istituto della verifica preliminare richiesta al Garante (ai sensi dell'art. 17, d.lgs. n. 196/2003) quando i trattamenti di dati di natura non sensibile presentavano rischi specifici per i diritti, le libertà fondamentali e la dignità dell'interessato.

Nel nuovo quadro normativo spetta direttamente al titolare del trattamento effettuare una "valutazione d'impatto sulla protezione dei dati" di ogni tipo di trattamento che presenti "un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35 del RGPD). L'Autorità di controllo potrà, d'altra parte, essere chiamata a rendere un "parere scritto" al titolare in relazione ai soli trattamenti che presentino rischi elevati che il titolare stesso non abbia "identificato o attenuato sufficientemente" attraverso l'adozione di misure adeguate (art. 36 del RGPD). Al riguardo, l'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati (art. 35, par. 4). Allo stato il Garante, nell'ambito del meccanismo di coerenza previsto dall'art. 63 del RGPD, ha individuato un elenco di trattamenti transfrontalieri da sottoporre a valutazione di impatto con provvedimento 11 ottobre 2018, n. 467 (doc. web n. 9058979); tale elenco non è esaustivo, restando fermo quindi l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati laddove ricorrano due o più dei criteri individuati dalle Linee guida in materia di valutazione d'impatto del 4 aprile 2017 elaborate dal Gruppo Art. 29, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (WP 248, rev. 01).

L'attività di individuazione dei rischi specifici da parte del titolare potrà e dovrà tener conto dei provvedimenti adottati dal Garante in sede di verifica preliminare, con i quali sono stati già valutati numerosi e complessi profili di rischio relativi a diverse tipologie di trattamenti di dati personali nell'ambito del rapporto di lavoro, specie di quelli effettuati con strumenti elettronici.

Si segnala che il Garante ha proseguito anche nel corso del 2018, in relazione a casi concreti dei quali si dà conto di seguito, l'attività applicativa ed interpretativa delle modifiche che hanno interessato la disciplina di settore in materia di controlli a distanza dell'attività del lavoratore (art. 4, l. n. 300/1970, espressamente richiamato dall'art. 114 del Codice).

Dati giudiziari

Tra le novità del RGPD che interessano in modo particolare l'ambito dei rapporti di lavoro si segnala la mutata disciplina relativa ai trattamenti dei dati giudiziari. L'art. 10 del RGPD prevede, infatti, che "il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'art. 6, par. 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati".

Il nuovo quadro normativo demanda quindi al legislatore l'individuazione delle ipotesi al ricorrere delle quali è consentito effettuare il trattamento di tale particolare tipologia di informazioni, nonché la predisposizione di "garanzie appropriate" a tutela degli interessati. Differentemente dal sistema previgente, pertanto, l'autorizzazione del Garante non costituisce più base giuridica idonea per effettuare tali trattamenti. L'autorizzazione generale al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici n. 7/2016 ha comunque cessato di produrre effetti giuridici alla data del 19 settembre 2018, in base all'art. 21,

comma 3, d.lgs. n. 101/2018 (posto che il comma 1 di tale disposizione non ha contemplato la relativa situazione di trattamento nel novero di quelle da sottoporre a verifica di compatibilità con il RGPD ed il decreto che ha modificato il Codice).

Coerentemente con tale prospettiva, l'art. 2-*octies* del Codice ha previsto che in mancanza di specifiche disposizioni di legge o di regolamento, i trattamenti dei dati giudiziari potranno avvenire in base a quanto sarà stabilito con apposito decreto del Ministro della giustizia, anche con riferimento alla "verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti" (v. art. 2-*octies*, comma 3, lett. *c*), del Codice).

Nelle more dell'adozione del menzionato decreto ministeriale il legislatore ha previsto che, oltre alle ipotesi già espressamente individuate da disposizioni normative, il trattamento dei dati giudiziari è consentito nel caso in cui costituisca specifica attuazione dei protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con le prefetture, sempre che sia stato acquisito il prescritto parere del Garante e che all'interno dei protocolli risultino specificati "la tipologia dei dati trattati e le operazioni eseguibili" (v. art. 22, comma 12, d.lgs. n. 101/2018).

13.3. *Il trattamento di dati relativi ai dipendenti tramite sistemi di geolocalizzazione*

Il Garante ha continuato ad occuparsi di trattamenti effettuati attraverso dispositivi che consentono la localizzazione geografica di veicoli e dispositivi *smartphone/tablet* e quindi, indirettamente, dei dipendenti cui gli stessi sono affidati per l'esecuzione della prestazione lavorativa. Sotto il profilo della conformità alla disciplina lavoristica sui controlli a distanza l'Autorità – avuto riguardo alla concreta configurazione dei sistemi tecnologici utilizzati, alle finalità perseguite e alle modalità di utilizzo dei sistemi – ha ritenuto, nei casi sottoposti alla sua attenzione (e di seguito sintetizzati), che i sistemi utilizzati non risultano "direttamente preordinati all'esecuzione della prestazione lavorativa" e pertanto devono essere qualificati strumenti dai quali "derivi anche la possibilità di controllo a distanza" (con conseguente applicazione dell'art. 4, comma 1, l. n. 300/1970).

Geolocalizzazione di veicoli aziendali

Nell'ambito delle attività di controllo svolte, rispettivamente, a seguito di una segnalazione e d'ufficio, l'Autorità ha disposto il divieto dell'ulteriore trattamento di dati riferiti ai dipendenti mediante l'utilizzo di un sistema di localizzazione dei veicoli ritenuto in violazione dei principi di necessità e proporzionalità rispetto alle finalità perseguite. In particolare, a fronte delle dichiarate esigenze organizzative e di sicurezza (efficiente gestione del parco veicoli; necessità di individuare rapidamente il veicolo più vicino in caso di richiesta di intervento; sicurezza dei dipendenti e dei beni aziendali; conseguimento di benefici in occasione della stipula di contratti di assicurazione) le caratteristiche del sistema consentivano al titolare, mediante il collegamento con la piattaforma web messa a disposizione dal fornitore del servizio, di visualizzare in tempo reale, attraverso la sezione "mappa", la posizione dei veicoli, il loro stato (fermo/in movimento), la velocità e dati ulteriori relativi all'utilizzo degli stessi (le ore di impegno e di guida, la velocità media, indicate sia in totale che distintamente per ciascuna tratta effettuata, nonché le pause, anche di pochi minuti). Tali informazioni sono risultate essere disponibili per un anno, congiuntamente alla mappa geografica dei percorsi effettuati giornalmente, unitamente alla possibilità di consultare *report* relativi all'attività dei singoli veicoli.

Al riguardo, il Garante ha ritenuto che gli scopi rappresentati dalla società avrebbero potuto essere utilmente e legittimamente perseguiti con la raccolta di informa-

zioni assai più limitate e conservate per un arco di tempo sensibilmente più ristretto, mentre il sistema – utilizzato nella versione standard senza alcuna modifica richiesta al fornitore – è risultato in concreto idoneo a realizzare il monitoraggio continuo dell'attività del dipendente, in violazione dei principi di necessità, pertinenza e non eccedenza (in relazione agli artt. 3 e 11, comma 1, lett. *d*) ed *e*), del Codice e 5, par. 1, lett. *c*) ed *e*), del RGPD). Inoltre, in applicazione dei principi e delle disposizioni poste dal RGPD, i titolari avrebbero dovuto configurare il sistema tecnologico con modalità tali da garantire che fossero trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (cfr. in proposito, oltre agli articoli sopra citati, anche l'art. 25 del RGPD, in attuazione del principio di cd. *privacy by default*).

Le caratteristiche del sistema sono state ritenute altresì non conformi alla disciplina lavoristica in materia di controlli a distanza, sì che anche da tale angolatura il relativo trattamento è risultato illecito, in quanto la richiamata disciplina "pure a seguito delle modifiche disposte con l'art. 23 del decreto legislativo 14 settembre 2015, n. 151, non consente l'effettuazione di attività idonee a realizzare il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore". Sotto tale ultimo profilo si segnala altresì che in relazione ad uno dei casi decisi dall'Autorità è risultato che la società titolare del trattamento consentiva l'utilizzo dei veicoli aziendali anche per esigenze di carattere personale, sì che l'attività di geolocalizzazione è risultata idonea a consentire il trattamento di dati "non rilevanti ai fini della valutazione dell'attitudine professionale" del dipendente (con conseguente violazione dell'art. 8, l. 20 maggio 1970, n. 300, Statuto dei lavoratori).

Il Garante ha ritenuto altresì, in sede di prima applicazione dei principi di minimizzazione dei dati e di *privacy by default* (artt. 5, par. 1, lett. *c*), e 25, del RGPD), di dover impartire alcune prescrizioni al fornitore del servizio di localizzazione utilizzato dalle società, relativamente alle informazioni da fornire ai propri clienti (che devono essere informati della possibilità di consentire la disattivazione del dispositivo attraverso la cd. funzione *privacy* e di modificare alcune impostazioni standard del servizio). Il fornitore del servizio dovrà inoltre configurare la stessa versione standard del servizio con modalità proporzionate in relazione al diritto alla riservatezza degli interessati, con particolare riferimento alla periodizzazione temporale della rilevazione della posizione geografica, ai tempi di conservazione dei dati e alla messa a disposizione e memorizzazione delle mappe dei percorsi effettuati (provv.ti 28 giugno 2018, n. 396, doc. web n. 9023246 e 19 luglio 2018, n. 427, doc. web n. 9039945).

Geolocalizzazione delle guardie particolari giurate

All'esito di un procedimento avviato con istanza di verifica preliminare prima del 25 maggio 2018, il Garante ha ammesso il trattamento prospettato da una società di vigilanza privata da effettuarsi mediante installazione di un applicativo, completo di funzionalità di localizzazione geografica, sui dispositivi *smartphone* o *tablet* consegnati alle guardie particolari giurate.

La decisione ha tenuto conto della particolarità dell'attività – soggetta ad una rigorosa disciplina – svolta dalla società nell'ambito dei servizi di cd. sicurezza complementare, anche in sede di valutazione della conformità dei trattamenti ai principi di necessità e proporzionalità. Ciò anche con riferimento alla periodizzazione temporale della rilevazione geografica dei dispositivi da parte del sistema, stabilita in 120 secondi, termine in sé assai ravvicinato ma ritenuto in concreto non in contrasto con i principi di protezione dei dati alla luce delle specifiche esigenze di sicurezza di persone e beni connesse con l'esercizio dell'attività di vigilanza. Tale valutazione ha altresì tenuto conto delle complessive caratteristiche del sistema, in particolare dei brevi tempi di conservazione dei dati di localizzazione raccolti (24 ore, salvo spe-

cifiche eccezioni previste dall'ordinamento) e della previa individuazione di eventi predeterminati al verificarsi dei quali i soggetti autorizzati possono visualizzare sui monitor della centrale operativa la posizione dei dispositivi.

Il Garante ha ritenuto necessario impartire alcune prescrizioni a tutela dei diritti degli interessati relative alla configurazione del sistema, quali l'oscuramento della visibilità della posizione geografica decorso un periodo determinato di inattività dell'operatore sul monitor; il posizionamento di un'icona sul dispositivo che indichi che la funzionalità di localizzazione è attiva; la previsione di un meccanismo che consenta la disattivazione della funzionalità di localizzazione durante le pause consentite dell'attività lavorativa (provv. 18 aprile 2018, n. 232, doc. web n. 9358266).

13.4. *Trattamenti mediante un sistema di videosorveglianza mobile*

Per la prima volta l'Autorità si è occupata di un sistema di videosorveglianza basato su dispositivi indossabili (cd. *body cam*) adottato, in via sperimentale (sei mesi), da una società privata (in relazione all'utilizzo di microcamere indossabili da parte di alcuni reparti mobili della polizia di Stato, si veda il parere 31 luglio 2014, doc. web n. 3423775).

In particolare l'utilizzo del sistema è stato prospettato all'Autorità nell'ambito di una verifica preliminare attivata da una società che fornisce servizi di trasporto pubblico locale su ferrovia, al fine di incrementare la sicurezza di utenti e dipendenti a fronte di reiterati episodi di aggressione e di danneggiamento avvenuti a bordo delle vetture. La necessità di utilizzare il sistema è derivata anche dalla rappresentata impossibilità tecnica di installare telecamere a bordo delle vetture ferroviarie di non recente costruzione. La società ha rappresentato di voler attivare le procedure previste dall'art. 4, comma 1, l. n. 300/1970.

Il sistema si compone di microcamere indossabili, da apporre sulla divisa di capitreno e personale addetto alla sicurezza, all'altezza della spalla, che si collegano con la centrale operativa al momento dell'attivazione da parte dell'operatore, esclusivamente al verificarsi di determinati eventi.

Il Garante ha ritenuto che tale particolare modalità di ripresa di immagini, rispetto ai tradizionali sistemi di videosorveglianza che utilizzano telecamere fisse, se da un lato consente una migliore qualità dell'immagine raccolta, in quanto più ravvicinata, d'altro canto offre una limitata visibilità del "contesto" in cui i fatti documentati si collocano. Inoltre il momento di inizio e fine delle videoriprese è demandato all'iniziativa dell'operatore che indossa il dispositivo, differentemente dai sistemi ad impianti fissi. Tale tipologia di sistema, pertanto, presenta rischi specifici per i diritti e le libertà fondamentali degli interessati – sia dipendenti che utenti del servizio di trasporto ferroviario –, anche di rilievo costituzionale (diritto alla riservatezza e alla protezione dei dati personali ex art. 2 Cost. e libertà di circolazione ex art. 16 Cost.).

L'Autorità ha quindi precisato che la decisione si intende riferita unicamente al trattamento avente le caratteristiche descritte nell'istanza. In caso di adozione del sistema a regime, posto il venir meno dell'istituto della verifica preliminare dopo il 25 maggio 2018, la società, in base al principio di responsabilizzazione di cui all'art. 24 del RGPD, oltre a verificare il rispetto di tutti i principi in materia, dovrà verificare in prima battuta la conformità alla disciplina vigente del trattamento che intende effettuare nonché valutare la necessità di procedere alla valutazione di impatto prevista dall'art. 35 del RGPD.

Con il provvedimento sono state impartite alla società alcune prescrizioni a

tutela dei diritti degli interessati, quali in particolare: l'indicazione all'interno di un disciplinare interno delle specifiche condizioni che legittimano l'attivazione dei dispositivi (prevedibile concreto pericolo di danni a persone e cose) nonché le modalità di utilizzo dei dispositivi stessi, prevedendo specifiche cautele da adottare nel caso in cui le riprese video coinvolgano soggetti "deboli" quali vittime di reati, testimoni, minori di età o riprendano luoghi assistiti da particolari aspettative di riservatezza (ad es., servizi igienici); la previsione di attività di verifica sulle immagini raccolte al fine di accertarne l'effettiva rilevanza rispetto alle finalità perseguite; il tracciamento delle operazioni di accesso ed estrazione dei dati raccolti; la predisposizione di misure affinché la funzionalità audio (ritenuta dalla stessa società non necessaria) non sia attiva; l'oscuramento delle immagini riferite a terzi non coinvolti dai fatti in caso di comunicazione delle immagini alle compagnie di assicurazione; l'adozione di misure volte a non consentire agli operatori che indossano i dispositivi operazioni di modifica, cancellazione e duplicazione delle immagini raccolte; la conservazione delle registrazioni video in forma cifrata; l'attivazione di strumenti comunicativi per avvisare gli utenti della presenza del sistema di videosorveglianza mobile e le sue principali caratteristiche, specificando anche che una spia accesa sul dispositivo indossabile indica che la funzionalità di videoripresa è attiva (provv. 22 maggio 2018, n. 362, doc. web n. 8995107).

13.5. *Controlli sulla posta elettronica aziendale*

Il Garante ha ribadito il proprio orientamento circa le condizioni di liceità dei trattamenti effettuati dal datore di lavoro sugli *account* di posta elettronica (di tipo individualizzato) assegnati al dipendente.

A seguito di un reclamo l'Autorità ha accertato che una società ha effettuato l'accesso al contenuto dei messaggi di posta elettronica scambiati dal reclamante con alcuni colleghi in un periodo di tempo significativo (alcuni mesi del 2015 e del 2016), utilizzandoli successivamente per effettuare una contestazione disciplinare. Tale attività è stata resa possibile dalla prassi aziendale consistente nella sistematica conservazione sul *server* aziendale di tutte le comunicazioni elettroniche spedite e ricevute sugli *account* assegnati ai dipendenti, per tutta la durata del rapporto di lavoro ed anche successivamente all'interruzione dello stesso. A tali dati la società si riservava di accedere avvalendosi di soggetti di volta in volta "autorizzati", anche in vista di futuri ed eventuali contenziosi nei confronti dei dipendenti, consentendo così alla società di precostituire elementi utili alla difesa in giudizio ed alla tutela dei propri diritti.

Sia il trattamento effettuato nei confronti del reclamante che, più in generale, la prassi adottata dall'azienda circa la gestione della posta elettronica aziendale è stata ritenuta non conforme alla disciplina posta in materia di protezione dei dati per una pluralità di profili. In primo luogo è risultato che i dipendenti non fossero stati (con documento individualizzato o attraverso la messa a disposizione di un disciplinare aziendale) informati delle specifiche modalità dei trattamenti effettuati sulla posta elettronica loro assegnata, come invece prescritto dalla normativa in materia di protezione dei dati (e ribadito nella materia specifica con le Linee guida per posta elettronica e internet, provv. 1° marzo 2007, n. 13, doc. web n. 1387522).

Sotto diverso profilo, l'Autorità ha ritenuto che non è conforme ai principi di liceità, necessità e proporzionalità del trattamento (v. artt. 3, 11, comma 1, lett. *a*) e *d*), del Codice) la conservazione per l'intera durata del rapporto di lavoro e successivamente all'interruzione dello stesso dei dati esterni e del contenuto di tutte le comunicazioni elettroniche scambiate dai dipendenti attraverso gli *account* azien-

dali, anche al dichiarato scopo di poter ricostruire gli scambi di comunicazioni tra gli uffici interni ed i rapporti intrattenuti con gli interlocutori esterni (clienti, fornitori, enti assicurativi).

La legittima necessità di assicurare l'ordinario svolgimento e la continuità dell'attività aziendale nonché di provvedere alla dovuta conservazione di documentazione in base a specifiche disposizioni dell'ordinamento è assicurata, in primo luogo, dalla predisposizione di sistemi di gestione documentale con i quali – attraverso l'adozione di appropriate misure organizzative e tecnologiche – individuare i documenti che nel corso dello svolgimento dell'attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore (in particolare dal d.P.C.M. 3 dicembre 2013, recante le regole tecniche in materia di sistema di conservazione ai sensi degli artt. 20, commi 3 e 5-*bis*, 23-*ter*, comma 4, 43, commi 1 e 3, 44, 44-*bis* e 71, comma 1, del Cad di cui al decreto legislativo n. 82 del 2005; parimenti i documenti che rivestano la qualità di "scritture contabili" devono essere memorizzati e conservati con modalità determinate: artt. 2214 c.c.; artt. 43 e 44, del Cad). I sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare tali caratteristiche.

Anche alla luce della richiamata disciplina emerge che la predisposizione di strumenti volti a garantire l'ordinaria ed efficiente gestione dei flussi documentali aziendali può ben essere perseguito con strumenti meno invasivi per il diritto alla riservatezza dei dipendenti e dei terzi.

Il Garante ha inoltre chiarito che il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti. Diversamente si eluderebbero le disposizioni poste con riguardo ai criteri di legittimazione del trattamento (su questo punto si vedano già i provv.ti 20 febbraio 2014, n. 91, doc. web n. 3115239; 19 marzo 2015, n. 173, doc. web n. 4039439; 4 giugno 2009, doc. web n. 1629029).

Del tutto diversa è l'ipotesi in cui il datore di lavoro metta a disposizione del dipendente l'archivio delle e-mail scambiate tramite l'*account* aziendale. Tale facoltà, che rientra tra le modalità di messa a disposizione degli strumenti di lavoro, può – se del caso – essere oggetto di specifiche istruzioni (ad es., individuando limiti temporali di conservazione anche diversificati in base alle funzioni svolte e coerenti con i limiti di spazio a disposizione e/o fornendo indicazioni sulla necessità di effettuare periodicamente la selezione e cancellazione dei messaggi conservati).

Inoltre, sotto il profilo della conformità alla disciplina lavoristica che costituisce autonomo criterio di liceità dei trattamenti, il Garante ha stabilito che la raccolta sistematica delle comunicazioni sugli *account* aziendali dei dipendenti in servizio, la loro memorizzazione per un periodo non predeterminato e comunque amplissimo e la possibilità per il datore di lavoro di accedervi per finalità indicate in astratto e in termini generali – quali la difesa in giudizio o il perseguimento di un legittimo interesse – costituisce attività di controllo dell'attività dei dipendenti.

La disciplina di settore in materia di controlli a distanza, come già osservato in precedenza con riferimento alla geolocalizzazione (cfr. le Linee guida per posta elettronica e internet cit., spec. par. 4, 5.2. lett. *b*) e 6; Consiglio di Europa, raccomandazione 1° aprile 2015, CM/Rec(2015)5, spec. princ. 14), pure a seguito delle modifiche disposte con l'art. 23, d.lgs. 14 settembre 2015, n. 151, non consente l'effettuazione di attività idonee a realizzare il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore (provv. 1° febbraio 2018, n. 53, doc. web n. 8159221).

13

13.6. *Trattamento di dati giudiziari*

Il RGPD, come indicato nell'introduzione al presente capitolo, ha adottato una disciplina più rigorosa in ordine al trattamento dei dati giudiziari. Il Garante, nell'imminenza della definitiva applicazione del RGPD (e prima dell'adozione del decreto legislativo n. 101/2018), ha approvato quattro decisioni di diniego a fronte di altrettante richieste di autorizzazione al trattamento di dati contenuti nel certificato del casellario giudiziale relativo ai dipendenti, ritenendo insussistente un'idonea base giuridica (legislativa o regolamentare) per l'effettuazione dei trattamenti richiesti. Non è stato ritenuto criterio di legittimazione idoneo la circostanza che (in due dei casi sottoposti all'Autorità) il trattamento sarebbe stato necessario per adempiere a quanto previsto in un contratto di fornitura di servizi, né che ai dipendenti dei titolari fosse applicabile un contratto collettivo nazionale che prevede tale trattamento. Ciò sia in considerazione della disciplina europea di imminente piena applicazione al momento dell'adozione dei provvedimenti, sia in ragione della ritenuta genericità del richiamo contenuto nel contratto collettivo, in quanto sprovvisto di alcun riferimento a specifiche esigenze di onorabilità legate allo svolgimento di determinati incarichi (in relazione ad un comparto che ricomprende una grande varietà di mansioni, in gran parte non connotate da una particolare delicatezza).

Inoltre in alcuni casi non risultava essere stata effettuata, in applicazione del principio di indispensabilità, l'individuazione del novero delle fattispecie penali ritenute rilevanti per la valutazione di idoneità del lavoratore allo svolgimento di specifiche attività. In uno dei casi è stata poi prospettata la comunicazione dei dati giudiziari ad un soggetto terzo (la stazione appaltante) in assenza, secondo quanto deciso dall'Autorità, di base giuridica.

Il Garante ha infine ritenuto che le prospettate modalità del trattamento, consistenti nella consegna del certificato del casellario giudiziale al datore di lavoro, avrebbero consentito la visibilità di tutti i dati contenuti nel certificato, nonostante la dichiarata delimitazione delle fattispecie di reato ritenute rilevanti ai fini della valutazione di idoneità allo svolgimento delle mansioni (provv.ti 22 maggio 2018, n. 314, doc. web n. 9005845; 22 maggio 2018, n. 315, doc. web n. 9005857; n. 316, doc. web n. 9005869; n. 317, doc. web n. 9001980).

13.7. *Trattamento di dati connesso all'utilizzo di dispositivi tecnologici*

Software* di gestione dei contatti con la clientela da parte di operatori di un *call center

All'esito di un procedimento avviato su reclamo, è emerso – anche attraverso l'effettuazione di accertamenti ispettivi – che una società ha utilizzato un sistema di Crm (*Customer Relationship Management*), preordinato alla gestione più efficiente dei contatti con la clientela, anche per trattare dati personali riferiti agli operatori addetti al *call center* (in particolare: l'identificativo del dipendente, il tipo di operazione svolta, la durata, la data e l'orario di conclusione della chiamata).

In primo luogo il Garante ha accertato che i dipendenti non erano stati informati, come previsto dall'ordinamento, delle specifiche operazioni di trattamento effettuate attraverso il sistema su dati personali a loro riferiti, con conseguente illiceità dei trattamenti effettuati (in base agli artt. 11, comma 1, lett. *a*) e 13 del Codice).

Nell'informativa era tuttavia presente il richiamo ad attività che presuppongono la raccolta di informazioni riferibili agli operatori (senza però che venisse data specifica evidenza), laddove la società si riservava di effettuare attività di controllo, in vista del successivo utilizzo dei dati raccolti mediante il sistema "per tutte le finalità

connesse al rapporto di lavoro" ai sensi e per gli effetti dell'art. 4, comma 3, l. n. 300/1970. In proposito il Garante ha ribadito che l'eventuale utilizzo dei dati raccolti ai sensi dell'art. 4, commi 1 e 2, l. n. 300/1970 per altri fini connessi alla gestione del rapporto di lavoro, attraverso ulteriori, successive operazioni di trattamento dei dati, presuppone il rigoroso rispetto del quadro normativo di riferimento, sia in materia di protezione dei dati, che in materia di controlli a distanza dei lavoratori (artt. 3, 11, comma 1, lett. *a*), *b*), *d*), ed *e*) e 13 del Codice nonché 4, comma 3, l. n. 300/1970; sul punto, v. provv. 24 maggio 2017, n. 247, doc. web n. 6495708, punto 5.3).

Con specifico riferimento alla conformità dei trattamenti alla disciplina in materia di controlli a distanza, l'Autorità ha altresì accertato che l'applicativo consente di risalire in ogni momento all'operatore che ha gestito il contatto telefonico con il cliente. Quindi il sistema non si limita a consentire la mera associazione tra la chiamata e l'anagrafica del cliente per facilitare l'attività di gestione della richiesta, ma permette l'effettuazione di "ulteriori elaborazioni" (es., memorizzazione di dati personali, anche degli operatori, ed estrazioni di *report*) da parte di diverse funzioni aziendali. In tal modo è possibile ricostruire, anche indirettamente, l'attività effettuata dagli operatori, di tal che il sistema è stato ritenuto idoneo a realizzare un controllo, anche solo potenziale e indiretto, dell'attività lavorativa, con conseguente applicazione dell'art. 4, comma 1, l. n. 300/1970, richiamato dall'art. 114 del Codice. Nel caso concreto tuttavia, pur essendo le finalità perseguite riconducibili ad esigenze organizzative e produttive, non risultano essere state attivate le garanzie procedurali prescritte dalla legge di cui la dichiarazione di illiceità del trattamento in esame anche sotto questo profilo (provv. 8 marzo 2018, n. 139, doc. web n. 8163433).

Utilizzo di sim aziendali

Nell'ambito di un procedimento di verifica preliminare relativa a dati riferiti all'utilizzo di schede sim aziendali affidate ai dipendenti (informazioni di dettaglio relative alle chiamate in uscita e, in alcuni casi – telefonate in *roaming* –, anche in entrata, sulla base della periodicità della fatturazione bimestrale), una società ha prospettato l'utilizzo di un sistema preordinato al controllo delle fatture del *provider* del servizio telefonico e all'analisi dell'andamento complessivo dei consumi con l'obiettivo di ridurre i costi aziendali, ottimizzare la qualità del servizio nonché individuare eventuali anomalie nei consumi.

Il Garante ha prescritto che i dati trattati debbano essere solo quelli necessari alle specifiche finalità del trattamento, e pertanto quelli idonei ad individuare specifiche voci di spesa nella fattura, in base al tipo di tariffazione prescelta. Non possono pertanto essere raccolti i dati in presenza di tariffe cd. *flat*, nonché le informazioni riferite a terzi nel caso di chiamate in entrata in *roaming*, quali il numero telefonico "chiamante", i dettagli della chiamata in entrata (giorno, ora dell'inizio della telefonata, durata della stessa) e il Paese di provenienza della chiamata stessa.

Non è stata inoltre ritenuta conforme ai principi di necessità, pertinenza e non eccedenza la commisurazione dei tempi di conservazione effettuata dalla società in dodici mesi, anche alla luce della specifica disciplina sulla conservazione dei dati relativi al traffico telefonico.

Quanto allo scopo di individuare eventuali consumi anomali, il Garante ha preso atto che, secondo quanto dichiarato, la società si limiterà a informare il *manager* del dipendente affinché questi provveda a invitarlo a contenere i costi e che i dati non saranno trattati per finalità disciplinari.

Il Garante ha ritenuto necessario prescrivere alla società l'adozione di un disciplinare interno relativo alle condizioni di utilizzo delle sim, nonché agli altri profili relativi ai trattamenti che si intendono effettuare. In ogni caso i numeri telefonici

relativi alle telefonate effettuate per esigenze personali non dovranno essere raccolti e, in proposito, dovrà essere predisposto un separato sistema di addebito e tariffazione. È stato altresì prescritto al titolare di adottare tecniche di cifratura dei dati estratti dal portale del fornitore del servizio di comunicazione elettronica e di anonimizzare i dati di fatturazione utilizzati al fine di analizzare l'andamento complessivo dei consumi in modo da valutare l'adeguatezza nel tempo del contratto con il *provider* (provv. 11 gennaio 2018, n. 3, doc. web n. 7554790).

Sistema di gestione delle chiamate *inbound*

Nell'ambito di un procedimento di verifica preliminare il Garante ha analizzato le modalità di funzionamento di un sistema (servizio di *speech analytics*), che consente di registrare le conversazioni telefoniche tra gli utenti e gli operatori dei *call center* (registrate in apposito *file* audio con modalità criptata), elaborando altresì ulteriori dati (mediante operazioni di "trascrizione" e di "indicizzazione semantico-ontologica"), allo scopo di generare *report* di sintesi utilizzabili per la rilevazione dei marcatori di qualità del servizio offerto.

Il sistema sarebbe altresì predisposto per depurare i dati raccolti da ogni elemento idoneo a identificare i soggetti partecipanti alle comunicazioni telefoniche, sia attraverso la rimozione di riferimenti diretti (nome e cognome del cliente) ed indiretti (ad es., numero di telefono dei clienti), attraverso un processo di cd. labelizzazione (sostituzione dei predetti riferimenti con "etichette" generali – ad es., "indirizzo" – nei *file* di testo e "silenzi" nei *file* audio). Il timbro vocale delle tracce audio verrebbe inoltre irreversibilmente alterato, in modo casuale, attraverso specifiche tecniche di *morphing*.

I dati raccolti non sarebbero altresì riconducibili agli operatori del *call center* bensì cumulativamente all'unità organizzativa di base ("modulo" o "*service team*": composta da 6 a 15 dipendenti). Inoltre il dato relativo alla singola postazione di lavoro sarebbe associata alla predetta unità organizzativa in maniera asincrona e cancellata entro 24 ore.

L'Autorità ha prescritto alcune misure a tutela degli interessati, in particolare la necessità di calcolare le percentuali di campionamento delle telefonate registrate e dell'ascolto delle conversazioni (rispettivamente pari al 10 e al 1,5%) su base giornaliera, quindi sul totale delle chiamate *inbound* e sul totale delle registrazioni effettuate per ciascuna giornata lavorativa. Fermo restando che, in ogni caso, le telefonate registrate per ciascuna unità organizzativa non possono superare il 20% delle telefonate gestite complessivamente nell'arco di un turno giornaliero dall'unità e che le registrazioni ascoltate non possono superare il 3% delle telefonate relative alla medesima unità organizzativa (provv. 18 aprile 2018, n. 229, doc. web n. 8987133).

13.8. *Comunicazione illecita di dati valutativi e disciplinari attraverso la pubblicazione sulla bacheca aziendale*

All'esito degli accertamenti avviati a seguito di una segnalazione presentata da alcuni soci lavoratori di una cooperativa che opera nel settore della logistica, il Garante ha vietato il trattamento dei dati effettuato mediante pubblicazione in bacheca aziendale di contestazioni e provvedimenti disciplinari, nonché delle valutazioni settimanalmente espresse dal consiglio di amministrazione su ciascun dipendente attraverso un giudizio di sintesi accompagnato da un *emoticon*. Il Garante ha ritenuto illecito il trattamento in relazione agli artt. 5, par. 1, lett. *a*) e *c*), 6 e 7 del RGPD considerato che la comunicazione mediante pubblicazione in bacheca di dati personali valutativi e disciplinari eccede il trattamento delle informazioni necessarie e pertinenti rispetto alla gestione del rapporto di lavoro in base a quanto previsto

dalle leggi, dai regolamenti e dalle disposizioni dei contratti collettivi applicabili o del contratto di lavoro individuale. Inoltre le concrete modalità di pubblicazione delle valutazioni settimanali attraverso l'affissione in bacheca riscontrate nel caso oggetto di segnalazione, sia per il fraseggio utilizzato che per l'idoneità a sottoporre costantemente all'osservazione dei colleghi le valutazioni sulla qualità del lavoro effettuato e sul corretto adempimento della prestazione della prestazione, anche attraverso una competizione premiale, sono state ritenute lesive della dignità personale, della libertà e della riservatezza dei lavoratori (provv. 13 dicembre 2018, n. 500, doc. web n. 9068983).

13.9. *Il trattamento di dati personali nel rapporto di lavoro pubblico: polizia locale e sistemi di localizzazione satellitare*

Nel nuovo quadro normativo spetta al titolare del trattamento effettuare una "valutazione d'impatto sulla protezione dei dati" di ogni tipo di trattamento che presenti "un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35 del RGPD), in merito alla quale il Garante potrà rendere un "parere scritto" al titolare quando il rischio non sia stato "identificato o attenuato sufficientemente" attraverso l'adozione di misure adeguate (art. 36 del RGPD). Al riguardo il titolare potrà fare riferimento all'ampia casistica contenuta nei provvedimenti adottati prima del 25 maggio 2018 dal Garante in sede di verifica preliminare (art. 17, d.lgs. n. 196/2003).

Entro questa cornice merita di essere menzionata una richiesta di verifica preliminare presentata da parte di un servizio di polizia locale gestito in forma associata tra più comuni, in relazione alle funzioni di polizia municipale e polizia amministrativa locale, rispetto al quale il Garante (provv. 29 marzo 2018, n. 181, doc. web n. 8576577) ha confermato il proprio orientamento ovvero ha considerato lecita (in quanto coerente con lo svolgimento dei compiti istituzionali attribuiti dall'ordinamento agli enti locali) l'installazione di un sistema di localizzazione satellitare sui veicoli e sulle radio ricetrasmittenti affidate alle squadre sul territorio. Rientrano in tale ambito anche le finalità di coordinamento del servizio per gestire situazioni di criticità o emergenza attraverso la consultazione delle informazioni sulla posizione geografica di veicoli e dispositivi da parte del personale autorizzato addetto alla centrale operativa. Parimenti lecito è stato ritenuto il trattamento consistente nella raccolta dei dati necessari alla rendicontazione delle attività effettuate dalle pattuglie nelle diverse aree comunali in vista della ripartizione tra i comuni associati dei costi sostenuti.

Poiché il sistema oggetto di valutazione consente tuttavia di ricostruire, anche indirettamente, l'attività degli operatori di polizia municipale, il Garante ha ricordato che il rispetto della disciplina di settore in materia di impiego di "strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori" costituisce condizione di liceità del trattamento (artt. 11, comma 1, lett. *a*), e 114 del Codice e art. 4, comma 1, l. n. 300/1970, come modificato dall'art. 23, d.lgs. n. 151/2015; sul punto, cfr. provv. 24 maggio 2017, n. 247, doc. web n. 6495708; v. pure Ispettorato nazionale del lavoro, circolare n. 2/2016 del 7 novembre 2016).

Anche con riferimento alla frequenza della rilevazione dei dati di geolocalizzazione, il Garante ha inteso ribadire il proprio orientamento in base al quale i sistemi devono essere configurati in modo da consentire la rilevazione del punto geografico con una periodizzazione temporale strettamente coerente con le finalità perseguite in quanto una rilevazione continuativa della posizione del veicolo dà luogo ad un

monitoraggio costante e ad un tracciamento del personale (in senso analogo, provv. 4 ottobre 2011, punto 3, cit. e, più di recente, provv. 16 marzo 2017, n. 138, doc. web n. 6275314 e provv. 24 maggio 2017, n. 247, doc. web n. 6495708, cit.; artt. 3 e 11, comma 1, lett. *a*) e *d*), del Codice; sul punto, raccomandazione 1° aprile 2015, CM/Rec(2015)5).

Nel caso di specie, preso atto delle particolari finalità perseguite nella attività di polizia locale per la gestione delle situazioni di criticità ed emergenza, si è tuttavia ritenuto che una rilevazione dei dati con una cadenza frequente non fosse in contrasto con i princìpi di pertinenza e non eccedenza dei dati trattati (art. 11, comma 1, lett. *d*), del Codice), come invece sarebbe in altri casi e per il perseguimento di diverse finalità. Ciò tenuto altresì conto, delle misure prospettate dal titolare a tutela degli interessati (quali la non identificabilità diretta degli operatori e la successiva eliminazione delle tabelle di assegnazione dei veicoli agli operatori) e delle assicurazioni fornite dallo stesso in merito al non utilizzo delle informazioni storicizzate per finalità diverse ed ulteriori rispetto a quelle della raccolta (quali la verifica della presenza degli operatori in un determinato luogo o per accertare le ore di lavoro effettuate o per finalità disciplinari).

13.10. *Il trattamento di dati giudiziari relativi ai messi notificatori*

Il Garante si è occupato del trattamento di dati giudiziari riferiti al personale dipendente degli operatori del settore postale da parte dell'ente pubblico affidatario del servizio di riscossione dei tributi. Nel corso dell'istruttoria è emerso che, in base al contratto di appalto, la società aggiudicataria, in qualità di fornitore del servizio di notifica (datore di lavoro e titolare del trattamento dei dati riferiti al proprio personale), provvedeva alla raccolta dei dati presso i propri dipendenti per poi trasmetterli ad Equitalia servizi di riscossione s.p.a., designata quale responsabile del trattamento. Sulla base della documentazione acquisita periodicamente dall'operatore del settore postale (l'elenco dei nominativi delle risorse che intendeva destinare al servizio e i relativi dati personali, anche giudiziari, nei termini sopra rappresentati), Equitalia provvedeva alla nomina dei messi e al rilascio del tesserino identificativo per lo svolgimento delle funzioni di notifica degli atti e delle cartelle di pagamento.

Dalla ricostruzione del quadro normativo applicabile è emerso che, in base alla disciplina di settore, la notifica delle cartelle di pagamento può avvenire mediante una pluralità di canali di notifica, tra i quali i cd. messi notificatori nominati dall'ente pubblico che assumono qualità di pubblico ufficiale (artt. 26, 49, comma 2 e 50, comma 2, d.P.R. n. 602/1973; art. 45, d.lgs. n. 112/1999). L'ente può anche procedere all'esternalizzazione dell'attività di notifica (differentemente da quella di riscossione) mediante affidamento del servizio ai vari operatori economici del settore postale (cfr. circolare Mef n. 105/E).

All'esito dell'istruttoria il Garante ha rilevato che la notificazione degli atti giudiziari (e, tra questi, le cartelle esattoriali: cfr. art. 14, l. n. 890/1982) è già consentita dall'ordinamento anche a mezzo del servizio postale (art. 149 c.p.c. e l. n. 890/1982). La disciplina applicabile al settore postale, in particolare quella concernente i titoli abilitativi per l'offerta al pubblico di servizi postali, prevede che debba essere "impiegato personale che non abbia riportato una condanna, con sentenza passata in giudicato, per delitto non colposo per il quale è prevista una pena detentiva non inferiore nel minimo a due anni o per uno dei delitti previsti nella sezione V, capo III, titolo XII, libro II, del codice penale" (art. 11 regola-

mento, all. A alla delibera n. 129/15/CONS dell'Agcom, ma, già artt. 4, comma 1, lett. *c*), d.m. 4 febbraio 2000, n. 75 e 3, comma 1, lett. *i*), d.m. 4 febbraio 2000, n. 73).

Tale normativa si riferisce allo svolgimento dei servizi postali tra i quali rientra, per espressa previsione normativa, anche la notifica degli atti giudiziari (e tra essi le cartelle di pagamento, in base all'art. 14, l. n. 90/1982). L'ordinamento, pertanto, già richiede in capo ai soggetti incaricati dell'espletamento del servizio postale l'insussistenza di particolari condizioni personali ostative alla fornitura del servizio secondo livelli di garanzia previsti dalla legge. Tali informazioni, in coerenza con la citata disciplina di settore, sono pertanto già in possesso del datore di lavoro che, nel caso di specie, è abilitato all'accesso al casellario giudiziario (ex artt. 28 e 39, d.P.R. 14 novembre 2002, n. 313). Le risultanze istruttorie hanno tuttavia evidenziato che la società/operatore del servizio postale non aveva reso una preventiva e completa informativa nei confronti del proprio personale destinato a svolgere tale servizio ed aveva richiesto ai propri dipendenti, per conto dell'ente pubblico concessionario del servizio della riscossione (Equitalia), dati giudiziari ulteriori rispetto a quelli che la citata disciplina di settore abilita a trattare, trasmettendoli a questo in assenza di un valido presupposto di liceità. Il Garante ha infatti chiarito che la disposizione del bando di gara o quella corrispondente contenuta nel capitolato tecnico dell'appalto predisposto da Equitalia, non può essere considerata un'idonea base normativa.

Riguardo ai trattamenti posti in essere da Equitalia riscossione s.p.a., anteriormente alla propria estinzione *ex lege* in data 1° luglio 2017, è stato chiarito che questi sono stati posti in essere per l'espletamento delle proprie funzioni istituzionali. Tra queste rientrano tutte le attività riconducibili alla notificazione delle cartelle e degli avvisi di intimazione mediante i messi notificatori e, quindi, anche le attività preordinate alla loro "nomina espressa" (cfr. art. 18, comma 2, Codice; art. 45, comma 2 e art. 50, d.lgs. n. 112/1999; art. 71, d.P.R. n. 445/2000 nonché, con riguardo alla esternalizzazione dell'attività di notifica, differentemente da quella della riscossione, la già citata circolare Mef (CiR) n. 105/E del 22.5.2000). In tale quadro, l'ente ha quindi operato in qualità di autonomo titolare del trattamento, non potendo ritenersi correttamente effettuata la designazione quale responsabile del trattamento da parte degli operatori postali e, per l'effetto, la raccolta e la conservazione dei dati giudiziari dei dipendenti della società postale (ancorché ai fini del rilascio dei tesserini) sono risultate essere effettuate in assenza di idoneo presupposto normativo.

Non è stata rinvenuta, infatti, neanche a cura dei soggetti coinvolti dall'istruttoria, una idonea base normativa in grado di definire i requisiti per l'accesso alle funzioni di messo notificare ai sensi dell'art. 45, d.lgs. n. 112/1999 e tale da legittimare il complessivo trattamento posto in essere. Né, contrariamente a quanto sostenuto nel corso del procedimento dalle parti, può essere invocato a tal fine l'art. 1, comma 159, l. n. 296/2007 in materia di messi notificatori comunali. Ciò in quanto, in presenza di trattamenti di dati giudiziari le norme applicabili devono essere soggette a principi di stretta interpretazione, non potendosi ricorrere all'analogia, in quanto sono richiesti, quali requisiti dei messi comunali, una specifica "qualifica professionale", "esperienza" "capacità" ed "affidabilità", ma non è presupposto il trattamento di dati giudiziari degli interessati da parte dell'amministrazione.

Alla luce dei rilievi sollevati dall'Autorità, l'ente pubblico ha cessato l'acquisizione dei dati giudiziari riguardanti i messi notificatori e il relativo trattamento ed ha dichiarato di voler implementare, per il futuro, una diversa procedura per il reclutamento e la designazione degli stessi conforme ai principi stabiliti dalla disci-

plina di protezione dei dati personali. È stato infatti ritenuto sufficiente, per tale finalità, acquisire apposita dichiarazione resa dai gestori del servizio postale che attesti di aver individuato il proprio personale da adibire al citato servizio nel rispetto dei limiti stabiliti dalla richiamata disciplina di settore (nota 28 febbraio 2018).

13.11. *Il trattamento di dati personali mediante sistemi di videosorveglianza*

A seguito di accertamenti *in loco* (nel caso di specie presso una sede territoriale dell'Agenzia delle dogane e dei monopoli), l'Autorità è poi tornata sul tema della videosorveglianza in contesti lavorativi pubblici, evidenziando alcuni profili di non conformità alla disciplina in materia di protezione dei dati personali.

Richiamando la giurisprudenza della Corte europea dei diritti dell'uomo, (caso Antovic e Mirkovic v. Montenegro Application n. 70838/13 del 28 novembre 2017), il Garante ha ribadito che il rispetto della "vita privata" deve essere esteso anche ai luoghi di lavoro pubblici, evidenziando che la videosorveglianza sul posto di lavoro pubblico può essere giustificata solo nel rispetto delle garanzie previste dalla legge nazionale applicabile, in mancanza delle quali costituisce un'interferenza illecita nella vita privata del dipendente. Tale ricostruzione e le conseguenti valutazioni in termini di liceità dei trattamenti sono coerenti anche con il quadro del RGPD che prevede per i trattamenti di dati effettuati nell'ambito del rapporto di lavoro che le disposizioni nazionali di settore assicurano "la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti", anche attraverso l'individuazione di "misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda […] i sistemi di monitoraggio sul posto di lavoro" (cfr. art. 88, par. 2). Nell'ordinamento italiano, il rispetto della disciplina di protezione dei dati, nell'ambito del rapporto di lavoro, si sostanzia anche dell'osservanza della rilevante disciplina di settore in materia di controlli a distanza dei dipendenti (art. 4, l. n. 300/1970, e art. 88, par. 2, del RGPD).

In particolare, con riguardo agli impianti audiovisivi il comma 1 del citato articolo, se da un lato circoscrive il campo delle finalità lecite (individuandole in quelle organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale), dall'altro richiede la stipulazione di un accordo con la rappresentanza sindacale unitaria o le rappresentanze sindacali aziendali, ovvero, in alternativa, l'autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro. Le esigenze di sicurezza rappresentate dal titolare, pure ritenute sussistenti nel caso di specie, non possono, di per sé sole, in base al quadro normativo nazionale, legittimare la presenza di tali dispositivi nei luoghi di lavoro pubblico. L'osservanza di tale disposizione, che non può essere soddisfatta dalla mera acquiescenza dei lavoratori o dal fatto che questi siano, di fatto, al corrente dell'esistenza del sistema in assenza delle citate garanzie (cfr. anche, Cass., III sez. pen., n. 22148/2017), costituisce, pertanto, condizione di liceità del trattamento dei dati personali, anche per effetto del rinvio operato dall'art. 114 del Codice.

Per tali ragioni il Garante ha rilevato, nel caso di specie, l'illiceità del trattamento (provv. 9 maggio 2018, n. 277, doc. web n. 8998303).

Con specifico riferimento all'eventuale visualizzazione "in tempo reale", anche da postazione remota, delle immagini già consultabili da parte del personale addetto alla portineria, il Garante ha sottolineato la necessità di valutare comunque la proporzionalità del trattamento alla luce dei principi di protezione dei dati (art. 5 del RGPD; cfr., in senso analogo, Ispettorato nazionale del lavoro, circolare 19

febbraio 2018, n. 5, indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e altri strumenti di controllo ai sensi dell'art. 4 della legge n. 300/1970, ove si legge che ciò può essere consentito "solo in casi eccezionali debitamente motivati").

13.12. *Il trattamento di dati personali idonei a rivelare l'adesione sindacale dei dipendenti*

A seguito di alcuni reclami, il Garante ha inoltre affrontato unitariamente la tematica del corretto trattamento dei dati personali dei dipendenti nell'ambito degli adempimenti che il datore di lavoro deve porre in essere per il versamento delle quote di iscrizione ad associazioni od organizzazioni sindacali su delega e per conto del lavoratore (cfr. anche art. 26, l. n. 300/1970 e provv. 18 dicembre 2014, n. 609, doc. web n. 3721603). Anche nel quadro del RGPD tali informazioni, relative all'adesione sindacale, costituiscono dati sensibili (ora denominate "categorie particolari di dati" dall'art. 9, par. 1, del RGPD) rispetto ai quali, in termini generali, sono vietati i trattamenti che non siano fondati su uno dei presupposti indicati dall'art. 9, par. 2, del RGPD. I trattamenti di dati sensibili effettuati per finalità di gestione del rapporto di lavoro (anche successivamente all'interruzione dello stesso) o in fase preassuntiva, possono essere effettuati solo in quanto necessari per l'adempimento di obblighi previsti da leggi e regolamenti oppure da un contratto collettivo nei limiti previsti dall'ordinamento (v. art. 9, par. 2, lett. *b*), del RGPD e il considerando n. 41). In ogni caso, il datore di lavoro tratta i dati dei propri dipendenti nel rispetto delle disposizioni nazionali "più specifiche per assicurare la protezione dei diritti e delle libertà dei lavoratori" (art. 88, par. 1, del RGPD).

Non diversamente dal quadro normativo previgente, le informazioni relative all'adesione al sindacato possono essere trattate da parte del datore di lavoro in adempimento degli obblighi correlati alla gestione del rapporto di lavoro previsto dalla legge o per adempiere agli obblighi derivanti dal rapporto di lavoro, ad esempio, per effettuare il versamento delle quote di iscrizione ad associazioni o organizzazioni sindacali su delega e per conto del dipendente (cfr. art. 88, par. 1 e 9, par. 2, lett. *b*), del RGPD).

Il datore di lavoro (nel caso di specie, un'azienda socio-sanitaria territoriale) non può tuttavia comunicare ad una organizzazione sindacale la nuova sigla alla quale ha aderito un suo ex iscritto. A giustificazione del proprio comportamento, l'azienda aveva affermato di aver ritenuto necessario informare la rappresentanza sindacale della variazione per evitare il rischio che, senza questa comunicazione, l'organismo continuasse ad operare in una composizione non più aderente alla realtà, con inevitabili ricadute sulla validità della contrattazione aziendale. Il Garante ha tuttavia rilevato che per consentire al sindacato di espletare le procedure che seguono la revoca dell'affiliazione sindacale e della relativa delega, il datore di lavoro avrebbe dovuto limitarsi a comunicare la sola scelta del lavoratore di non aderire più all'originaria sigla di appartenenza. Nel caso di specie invece l'amministrazione non si era limitata a comunicare alla rappresentanza sindacale interessata la revoca dell'affiliazione da parte di alcuni lavoratori ma aveva inviato, a tutti i componenti della citata sigla sindacale, una e-mail recante in allegato documenti nei quali era espressamente indicata la contestuale iscrizione dei predetti ad altro sindacato dando luogo, così ad un'illecita comunicazione di dati personali sensibili dei reclamanti (cfr. *newsletter* 7 dicembre 2018, doc. web n. 9065999).

13.13. *Il trattamento di dati personali relativi alle condizioni di salute dell'interessato nell'ambito dell'amministrazione militare*

Il Garante ha definito un reclamo relativo al trattamento dei dati personali relativi alla salute di un dipendente mettendo in evidenza come il mancato rispetto di quanto disposto dalla disciplina di settore applicabile avesse determinato altresì un trattamento illecito dei dati di un appartenente all'amministrazione militare, sia nel procedimento per il riconoscimento della dipendenza dell'infermità da causa di servizio, sia nell'ambito della gestione della certificazione medica nel corso dell'assenza dal servizio per malattia.

Con riguardo al primo profilo è emerso che la competente commissione medica aveva redatto il verbale di visita medica conformemente a quanto disposto dall'art. 7, comma 4, d.m. economia e finanze 12 febbraio 2004, trasmettendone copia all'amministrazione di appartenenza ai sensi dell'art. 7, comma 1, d.P.R. n. 461/2001. Questa aveva, a propria volta, trasmesso tutta la documentazione ad altre articolazioni territoriali, presso le quali il reclamante era stato in servizio in precedenza, perché procedessero alla "notifica all'interessato".

La normativa di settore (adottata ai sensi dell'art. 22, comma 3-*bis*, l. n. 675/1996, e, quindi, ai sensi dell'art. 20 del Codice) stabilisce tuttavia forme e modalità per la notifica degli atti del procedimento all'interessato (art. 13, commi 3 e 4, d.P.R. n. 461/2001), in coerenza con il quadro normativo in materia di protezione dei dati personali (sia con quello applicabile al caso di specie, sia con quello delineatosi a seguito dell'entrata in vigore del RGPD) nonché con le indicazioni fornite nel tempo dal Garante circa la necessaria adozione di specifiche cautele nell'ambito delle comunicazioni al lavoratore – effettuate per il tramite di personale incaricato di talune operazioni di trattamento – tra le quali, in particolare, l'adozione di forme di comunicazione individualizzata al fine di prevenire la conoscibilità di dati personali, specie se sensibili o giudiziari, da parte di soggetti diversi dal destinatario (cfr. Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, provv. 14 giugno 2007, doc. web n. 1417809). In tale quadro, l'inoltro per via gerarchica di tutta la documentazione medica mediante posta elettronica a una pluralità di articolazioni territoriali, rispetto alle quali non è stata comprovata la competenza in ragione delle rispettive funzioni, ha determinato un trattamento di dati che il Garante ha valutato non conforme alla disciplina di protezione dei dati e all'art. 13, comma 4, d.P.R. n. 461/2001.

Sotto altro profilo, è stato altresì accertato che un certificato medico recante indicazione relativa alla diagnosi era stato trattato in contrasto con quanto previsto dalla disciplina applicabile al personale militare mediante il sistema del cd. doppio certificato. L'art. 748 delle disposizioni regolamentari in materia di ordinamento militare (d.P.R. 15 marzo 2010, n. 90) prevede, infatti, che il militare, assente per motivi di salute, trasmetta un certificato medico, con la sola prognosi, al superiore diretto e un ulteriore certificato medico, recante sia la prognosi che la diagnosi, al competente organo della sanità militare, affinché nell'esercizio delle funzioni del servizio sanitario militare (previste dall'art. 181, d.lgs. 15 marzo 2010, n. 66, Codice dell'ordinamento militare) sia consentita la verifica della persistenza dell'idoneità psicofisica ad attività istituzionali connesse alla detenzione o all'uso delle armi, ovvero comunque connotate da rischio o controindicazioni all'impiego. A tali diposizioni ha dato successivamente attuazione il d.m. Ministero della difesa 24 novembre 2015 che disciplina le modalità di adozione del sistema del cd. doppio certificato specificando gli accorgimenti volti a far in modo che, nell'ambito della trasmissione con

modalità non digitali della predetta certificazione medica, il certificato, recante anche la diagnosi, sia destinato unicamente agli organi sanitari militari competenti e non confluisca nel fascicolo personale del militare (cfr. art. 4, comma 3, d.m. cit.; v. anche circolare 22 marzo 2017, nr. 108/125-18-1-1975 e circolare 6 aprile 2017).

Nel caso di specie è stato invece accertato che il certificato, contenente anche la diagnosi, era stato trasmesso dal comando presso il quale prestava servizio l'interessato non solo all'infermeria presidiaria ma anche ad altri quattro comandi. È stato, pertanto, ritenuto che il trattamento dei dati del reclamante non fosse avvenuto nel rispetto della disciplina di protezione dei dati e del quadro normativo di settore essendo stati resi edotti della diagnosi del dipendente, non solo gli organi della sanità militare (nel caso di specie l'infermeria presidiaria), ma anche altre articolazioni amministrative non autorizzate, rispetto alle quali era stato successivamente disposto dall'amministrazione di provvedere a "cancellare la diagnosi" e di "distruggere il certificato medico, eventualmente allegato" (nota 12 gennaio 2018).

14 Le attività economiche

14.1. *L'implementazione del RGPD nel contesto produttivo*

Dialogo e confronto con le associazioni di categoria

L'avvicinarsi, nel corso del 2018, della data di piena operatività delle nuove norme regolamentari ha creato attenzione e preoccupazione nel mondo imprenditoriale, moltiplicando l'invio di quesiti e richieste di parere, accompagnati da richieste di incontro con l'Ufficio al fine di sottoporre le questioni ritenute più rilevanti e problematiche nel rispettivo ambito di interesse.

È iniziata così un'intensa fase di dialogo e confronto con un'ampia schiera di associazioni di categoria (alcune aventi già da tempo relazioni con l'Autorità, altre che per la prima volta hanno preso contatto con gli uffici) realizzando diverse occasioni di incontro che hanno visto la presenza di associazioni quali Confindustria, Abi, Ania, Confartigianato, Confcommercio, Cna, Confapi, vale a dire le rappresentanze più ampie del mondo dell'industria, dell'artigianato, del commercio, delle banche e delle assicurazioni. Ad esse si sono affiancate altre associazioni di settore che hanno permesso all'Ufficio di inquadrare le disposizioni generali in contesti particolari, spesso caratterizzati da una peculiare normativa settoriale e da specifiche problematiche applicative. Basti pensare ai temi affrontati con Assorevi (revisori ufficiali dei conti), Assaeroporti (società di gestione aeroportuale), Assolavoro (agenzie di lavoro), Asstel (operatori telefonici e telematici), Unirec (operatori del recupero crediti), Univigilanza (società di vigilanza privata), Ancic (società di informazione commerciale), Asstra (aziende di trasporto pubblico locale).

Altrettanto significativa è stata la partecipazione dell'Ufficio a iniziative pubbliche esterne che hanno visto, in alcune occasioni, la presenza di centinaia di rappresentanti delle più svariate realtà imprenditoriali.

A queste occasioni di carattere più generale, si sono poi affiancate, a partire dalla seconda metà dell'anno, gli incontri, più mirati e specifici, avvenuti su richiesta dei neonominati Rpd di alcune importanti realtà societarie (Fca Group, Rai, Poste italiane, Enel, Unicredit, Intesa Sanpaolo, Cerved ecc.). Sono state occasioni preziose per una prima verifica "sul campo" del funzionamento delle nuove disposizioni e per cogliere suggestioni e richieste di chiarimento che potranno ispirare l'attività dell'Ufficio nei prossimi mesi.

FAQ sul Rpd in ambito privato

A partire dal 25 maggio 2018 si è manifestata come urgente l'esigenza di dare risposta agli interrogativi posti all'Autorità circa la figura del Rpd (altrimenti noto con l'acronimo inglese Dpo, *Data protection officer*).

A tale scopo il 23 marzo 2018 l'Autorità ha pubblicato sul proprio sito istituzionale la pagina inerente le nuove FAQ sul Rpd in ambito privato, in aggiunta a quelle adottate dal Gruppo Art. 29 in allegato alle Linee guida sul Responsabile della protezione dei dati (doc. web n. 8036793).

In tale sede i principali interrogativi affrontati dal Garante hanno avuto ad oggetto (i) le caratteristiche soggettive della figura del Rpd, in particolare mediante puntuali riferimenti ai compiti previsti dall'art. 39 del RGPD; (ii) l'individuazione delle categorie di soggetti privati obbligati alla sua designazione e di quelle per le quali tale scelta, per quanto raccomandata anche dal Gruppo Art. 29, rimane

FAQ sul Registro dei trattamenti

opzionale; (iii) gli interrogativi circa le possibili declinazioni discendenti dalla nomina del Rpd nel tessuto imprenditoriale, in particolare, la possibilità di nomina di un unico Rpd nell'ambito di un gruppo imprenditoriale, o la possibilità di nominare a tale incarico un soggetto esterno; (iv) le cause di incompatibilità con altri incarichi.

Nell'ottobre 2018, il Garante ha poi pubblicato sul proprio sito istituzionale una serie di FAQ in materia di Registro dei trattamenti idonee a fornire più puntuali indicazioni in ordine agli interrogativi più significativi relativi all'utilizzo del suddetto Registro, ai soggetti tenuti a redigerlo, al contenuto dello stesso, alle modalità della sua redazione. A tal fine il Garante ha predisposto, in allegato alle FAQ, due modelli di registri semplificati riferiti rispettivamente al titolare del trattamento ed al responsabile.

È stato chiarito, in particolare, cosa sia il Registro dei trattamenti e quali le informazioni che in esso devono essere contenute.

Per quanto concerne, in particolare, l'individuazione dei soggetti tenuti a redigere il suddetto Registro, il Garante ha proposto in sede europea un'interpretazione dell'art. 30, par. 5, del RGPD idonea ad esentare da tale obbligo la categoria, molto diffusa nel tessuto economico italiano, delle piccole e medie imprese ovvero ha suggerito di configurare la deroga ogniqualvolta, a seguito della concreta valutazione del rischio da parte del titolare del trattamento, ricorrano tutte le condizioni elencate all'art. 30, par. 5 (rischio per i diritti e le libertà dell'interessato, trattamento non occasionale, trattamento avente ad oggetto categorie particolari di dati, sensibili o giudiziari). Il confronto con le autorità di controllo europee ha portato, invece, ad un orientamento più restrittivo della norma in questione che considera sussistente l'obbligo di tenuta del Registro in tutti i casi in cui sia presente già solo una delle condizioni sopra elencate. Peraltro è stata prevista, nel caso in cui il titolare tratti una sola categoria di dati, la possibilità di utilizzare un registro redatto in modo semplificato.

14.2. *Il settore bancario*

Nel corso del 2018 il numero di segnalazioni, reclami, quesiti e richieste di parere pervenute all'Autorità in materia di trattamento di dati personali effettuato da banche, società finanziarie, sistemi di informazione creditizia, Centrale dei rischi gestita dalla Banca d'Italia, Centrale di allarme interbancaria, concessionari di pubblici servizi (in particolare Poste italiane s.p.a.) ha registrato un *trend* in costante ascesa, a conferma della particolare criticità del settore.

Un numero molto consistente di esse ha riguardato profili sui quali il Garante si è già espresso in passato, tra l'altro con le Linee guida adottate il 25 ottobre 2007 (provv. 25 ottobre 2007, n. 53, doc. web n. 1457247) e con il provvedimento generale recante prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (provv. 12 maggio 2011, n. 192, doc. web n. 1813953), i cui princìpi risultano pienamente compatibili con il nuovo quadro regolatorio introdotto dal RGPD e dal decreto legislativo n. 101/2018.

In particolare, alcune di esse hanno riguardato il trattamento dei dati personali effettuato dagli istituti di credito in occasione delle operazioni di adeguata verifica della clientela prescritte dalla vigente normativa in materia di antiriciclaggio. Su tale complessa e delicata disciplina, peraltro, il Garante aveva avuto modo di esprimersi già nel 2017, rendendo il proprio parere (provv. 9 marzo 2017, n. 125, doc. web n. 6124534) sullo schema di decreto legislativo adottato dal legislatore nazionale in attuazione alla direttiva (UE) 2015/849 del Parlamento e del Consiglio del 20 mag-

gio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (cd. quarta direttiva). Sempre sulle variegate questioni affrontate dal Garante con le Linee guida del 2007, sono state esaminate e definite numerose istanze, in particolare, sui profili dell'accesso ai dati personali contenuti in rapporti bancari (di norma, libretti di risparmio, conti correnti e depositi titoli) riferiti a persone decedute, della richiesta di copia di documentazione riferita a rapporti bancari e della comunicazione a terzi di dati inerenti clienti.

Di particolare interesse per il settore, sotto altro profilo, sono stati gli approfondimenti curati dall'Ufficio in relazione al tema della compatibilità tra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 (cd. PSD2) e il RGPD. Al riguardo, anche all'esito di incontri istituzionali tenutisi presso il Ministero dell'economia e delle finanze con alcuni degli attori coinvolti, l'Autorità, su impulso dell'Abi, ha provveduto a fornire indicazioni e chiarimenti in argomento ad alcuni Ministeri e al Presidente del Consiglio dei ministri (v. nota 9 gennaio 2018, doc. web n. 9104322).

14.3. *Dai codici di deontologia nel settore economico e finanziario ai codici di condotta*

Già dai primi anni di vigenza del decreto legislativo n. 196/2003 il Garante ha dedicato una grande attenzione ai profili di protezione dei dati personali connessi all'attività dei sistemi di informazioni creditizie e a quelli delle società che si occupano di informazioni commerciali.

In tale prospettiva, l'Autorità si era fatta carico di promuovere la redazione di due importanti codici di deontologia e di buona condotta, ai sensi dell'art. 12 del Codice, quali utili strumenti per assicurare un'efficace disciplina di dettaglio rispetto alla mole di dati trattati ordinariamente in tali ambiti.

La scelta si è dimostrata lungimirante perché sia il cd. codice Sic (in vigore da maggio 2005), sia il più recente codice di deontologia in materia di trattamento dei dati personali a scopo di informazione commerciale (in vigore dall'ottobre 2015) hanno dimostrato di essere un equilibrato strumento di contemperamento dei molti, diversi e, a volte, contrapposti interessi in gioco, contribuendo ad assicurare certezza del diritto in un ambito delicato della nostra realtà economica e finanziaria. Proprio il ruolo efficace svolto da questi strumenti, riconosciuto da tutti gli interessati, ha ispirato la ricerca di un percorso normativo volto a salvaguardare il nocciolo duro (cioè le disposizioni essenziali su tipologie di dati trattati, meccanismi di inserimento, tempi di conservazione) dei vecchi codici e a "traghettarli" o meglio trasformarli e rifonderli in un nuovo abito normativo (il codice di condotta di cui agli artt. 40 e 41 del RGPD) coerente con il nuovo assetto regolamentare eurounitario.

Questa è in estrema sintesi la genesi e la ragione dell'art. 20, commi 1 e 2, d.lgs. n. 101/2018. Tali disposizioni guidano questo processo di trasformazione, assicurando *medio tempore* (fino ad un termine massimo di 12 mesi dalla data di entrata in vigore del citato decreto legislativo n. 101/2018, il 19 settembre 2018) la persistente vigenza dei predetti codici di deontologia e di buona condotta (all. A5 e A7 del Codice).

In questo arco di tempo le associazioni e gli altri organismi rappresentativi delle categorie interessate dovranno sottoporre (entro i primi sei mesi) al vaglio del Garante, che dovrà pronunciarsi in merito (entro i sei mesi successivi), una bozza di codice di condotta che, nel rispetto del sopra citato RGPD, riproponga ed eventualmente aggiorni i contenuti degli allegati A5 e A7 del decreto legislativo n. 196/2003.

Si tratta di operazione complessa (visto che deve tener conto anche di alcune modifiche legislative e di alcuni nuovi orientamenti interpretativi nel frattempo emersi), attualmente in corso, che potrà vedere la sua conclusione nel primo semestre del 2019.

14.4. *La videosorveglianza in ambito privato*

I profili di protezione dei dati personali connessi all'utilizzo di impianti di videosorveglianza sono tradizionalmente oggetto ogni anno di un consistente numero di segnalazioni e reclami che dimostrano una particolare sensibilità dell'opinione pubblica a questa tipologia di trattamenti sia quando vengono utilizzati in ambito domestico, sia quando sono installati in contesti imprenditoriali o condominiali.

Inoltre, prima della piena applicabilità delle nuove disposizioni regolamentari, sono stati sottoposti all'Autorità, in ottemperanza al disposto del noto provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680), numerose istanze di verifica preliminare incentrate su ipotesi di videosorveglianza cd. intelligente o comunque basate sull'utilizzo di meccanismi di ripresa particolarmente invasivi e potenzialmente lesivi dei diritti di utenti, dipendenti, ecc.

Ad esempio, con provvedimento 18 gennaio 2018, n. 13 (doc. web n. 7968051) il Garante ha autorizzato Costa Crociere s.p.a. alla conservazione delle immagini registrate dal sistema di videosorveglianza già installato a bordo delle navi della flotta.

Alla base della richiesta di prolungamento del termine di conservazione delle immagini fino a 14 giorni vi era l'esigenza di rafforzare il livello di tutela delle persone, del patrimonio e dei beni aziendali. Alcuni eventi (si pensi, in particolare, ai casi di scomparsa di persone durante la navigazione) hanno, infatti, portato a considerare l'allungamento dei tempi di conservazione delle immagini come uno strumento utile a consentire alla società e alle autorità competenti di acquisire elementi per l'identificazione dei trasgressori o, comunque, per la ricostruzione di tutto ciò che accade su una nave durante l'intera durata della crociera.

L'Autorità ha poi accolto, con provvedimento 5 aprile 2018, n. 198 (doc. web n. 8983828), la richiesta di verifica preliminare presentata da Philips Saeco s.p.a., avente ad oggetto l'attivazione di videocamere intelligenti e l'estensione dei tempi di conservazione delle immagini rilevate dall'impianto di videosorveglianza installato presso il proprio sito produttivo. La società, facente parte del gruppo multinazionale Philips e specializzata nella progettazione, creazione, produzione, e distribuzione di apparecchi elettrodomestici, elettrici ed elettronici sia per il mercato interno sia per il mercato internazionale, ha deciso di potenziare i sistemi di sicurezza esistenti e di installare un impianto di videosorveglianza finalizzato alla tutela del personale dipendente e del patrimonio aziendale; ciò anche a fronte delle richieste di implementazione di nuove misure di sicurezza da parte del gruppo di appartenenza al fine di poter includere il sito produttivo italiano tra quelli certificati per l'esportazione, secondo procedure in linea con gli standard di sicurezza elaborati dall'Organizzazione mondiale delle dogane (*World customs organization*).

Con provvedimento 18 aprile 2018, n. 234 (doc. web n. 8995078) il Garante ha valutato congruo il tempo di conservazione delle immagini rilevate dal sistema di videosorveglianza di Gardaland s.r.l. La società, proprietaria del parco divertimenti, dell'acquario Sea Life e dei complessi alberghieri situati in prossimità del parco, con-

trolla un'area complessiva di circa 600.000 mq che registra una media di 12.000 visitatori al giorno.

La richiesta di poter conservare fino a 30 giorni le immagini registrate dal sistema di videosorveglianza si basava su oggettive esigenze di sicurezza correlate non solo all'emergenza terrorismo e alla peculiare attività che si svolge all'interno della struttura, ma anche alla sua superficie molto estesa.

Il Garante, con provvedimento 9 maggio 2018, n. 273 (doc. web n. 8998311), ha anche accolto l'istanza di verifica preliminare presentata da Banca monte dei paschi di Siena s.p.a. relativa alla sperimentazione di soluzioni innovative che si avvalgono delle tecnologie di videoanalisi e di audiosorveglianza per la sicurezza delle filiali. L'adozione di sistemi intelligenti, basati sull'utilizzo di componenti audio e video integrati, in correlazione agli altri dispositivi già presenti nelle agenzie, consentirà alla banca di rilevare situazioni anomale e di prevenire significativamente il rischio di eventi criminosi, rendendo ancor più effettiva la sicurezza dei dipendenti e dei clienti.

Con provvedimento 22 maggio 2018, n. 364 (doc. web n. 9022264) il Garante ha infine accolto la richiesta di verifica preliminare presentata da Sperlari s.r.l. in relazione all'utilizzo presso il proprio stabilimento produttivo di un dispositivo di sicurezza – dotato di tecnologia Gps e collegato ad una piattaforma web di localizzazione e gestione allarmi – in grado di rilevare, in caso di segnalazione d'emergenza, la posizione dei lavoratori che operano in solitaria in aree dello stabilimento che presentano elevati rischi specifici per la salute e la sicurezza dei dipendenti.

14.5. *Automatizzazione dei sistemi di esazione dei pedaggi autostradali*

Autostrada pedemontana lombarda

Con provvedimento 22 maggio 2018, n. 361 (doc. web n. 9022076) il Garante ha preso in esame una richiesta di verifica preliminare relativa al trattamento di dati personali connessi all'implementazione di un sistema di esazione dei pedaggi autostradali, al momento unico in Italia, privo di barriere fisiche, basato sulla rilevazione automatica del numero di targa dei veicoli in transito – tramite telecamere posizionate sui cd. portali – e sul tracciamento dei percorsi effettuati.

Il sistema proposto (denominato *multilane free flow*), che comporta la trasmissione di immagini dai predetti portali ad un sistema centrale attraverso protocolli di comunicazione sicuri, prevede che, nel rispetto dei princìpi generali in materia di protezione dati e, in particolare, dei princìpi di necessità e di proporzionalità, da un lato le telecamere siano orientate in modo da evitare la ripresa diretta dei volti del conducente e degli eventuali passeggeri e, dall'altra, che le immagini siano conservate per un arco temporale fissato da un minimo di 48 ore (in caso di transito con *on board unit*) fino ad un massimo di tre mesi dall'avvenuto pagamento del pedaggio (in caso di transito senza *on bord unit*).

È inoltre consentito agli utenti effettuare il pagamento dei pedaggi anche tramite funzionalità *online* (servizio "conto targa", servizio ricaricabile e servizio "paga il pedaggio") previa registrazione al sito web della società e conseguente indicazione del/i numero/i di targa. Il sistema è congegnato in modo tale che, mentre il solo pagamento può essere eventualmente effettuato anche da un soggetto diverso dal proprietario dell'automezzo per l'ammontare complessivo dei pedaggi effettuati dal veicolo da lui indicato, tale utilizzatore del veicolo non può invece venire a conoscenza del dettaglio dei transiti effettuati (tratta, relativo giorno e ora), salva specifica autorizzazione da parte del proprietario.

La società, nel descrivere il sistema *free flow*, ha peraltro evidenziato come lo

stesso, oltre a determinare diversi effetti positivi per gli utenti dei percorsi autostradali tra cui maggiore scorrevolezza del traffico, riduzione dell'inquinamento e innalzamento dei livelli di sicurezza si pone in linea con il quadro normativo delineato in sede comunitaria (direttiva 2004/52/CE sull'interoperabilità dei sistemi di telepedaggio stradale) e con la stessa normativa italiana che all'art. 176, comma 11, del Nuovo codice della strada (decreto legislativo n. 285/1992) dispone che "l'esazione del pedaggio può essere effettuata mediante modalità manuale o automatizzata, anche con sistemi di telepedaggio con o senza barriere".

L'Autorità, quindi, nel valutare positivamente le finalità sopra rappresentate, prendendo atto dell'impossibilità di acquisire il consenso degli interessati in una fase antecedente all'effettivo utilizzo del tratto autostradale, in applicazione della disciplina sul cd. bilanciamento di interessi (art. 24, comma 1, lett. *g*), d.lgs. n. 196/2003) ha autorizzato i trattamenti di dati personali connessi al sistema *free flow* indipendentemente dal consenso degli interessati e, al contempo, ha individuato alcune misure di sicurezza aggiuntive rispetto a quelle descritte dalla società.

Aiscat

Il Garante si è inoltre pronunciato (provv. 22 maggio 2018, n. 318, doc. web n. 9009360) in ordine al trattamento di dati personali derivante dal prospettato utilizzo di un sistema di rilevazione dei veicoli in transito sull'intera rete autostradale per finalità di commisurazione del pedaggio al percorso realmente effettuato dagli utenti, oltre che a scopo di prevenzione e contrasto di eventuali condotte irregolari.

Il sistema sottoposto all'attenzione dell'Autorità, in grado di acquisire informazioni relative ai veicoli in transito lungo le tratte autostradali attraverso "portali" ubicati ai caselli di ingresso e di uscita e in punti "strategici" della rete (corrispondenti ai punti geografici che consentono un'alternativa di percorso), consentirebbe alle società proponenti (rappresentate dall'associazione di categoria) di adeguare il "vecchio" sistema di tariffazione del pedaggio autostradale alla normativa comunitaria in materia di telepedaggio (direttive 1999/62/CE del 17 giugno 1999 e 2004/52/CE), superando così alcune "criticità" evidenziate al riguardo dalla Commissione europea. Inoltre, il sistema permette di prevenire e accertare, sulla base dell'apposita disciplina di settore (art. 176, d.lgs. n. 285/1992), eventuali violazioni all'obbligo di pagamento del pedaggio. Con il nuovo sistema sarà così possibile ricostruire (e quindi commisurare il pedaggio dovuto) il percorso effettivamente compiuto, superando l'attuale meccanismo che, in caso di alternative di percorso, si basa su tariffazioni forfettarie.

A fronte di una prima pronuncia (negativa) adottata sulla base delle informazioni inizialmente fornite, le società proponenti si sono attivate per meglio rappresentare e documentare le esigenze di "monitoraggio" del traffico veicolare sottese all'istanza presentata all'Autorità, fornendo compiuti ragguagli anche in ordine ai ruoli *privacy* rivestiti da alcune delle società coinvolte (con funzioni essenzialmente tecniche) nell'iniziativa. Il Garante, preso atto degli ulteriori chiarimenti e della documentazione aggiuntiva prodotta, ha valutato – questa volta con favore – il trattamento sottoposto al proprio vaglio, ritenendolo motivato sulla base delle normative richiamate (art. 11, comma 1, del Codice) e rispondente a un legittimo interesse dei titolari.

14.6. *Verifiche preliminari*

Aeroporti di Roma s.p.a.

Con provvedimento 15 marzo 2018, n. 155 (doc. web n. 8789277) il Garante ha esaminato una istanza di verifica preliminare proposta dalla società Aeroporti di Roma, in merito all'utilizzo di un sistema di rilevazione delle immagini dotato di un

software che permette il riconoscimento della persona. Si tratta di un trattamento piuttosto ampio di dati biometrici connessi, in particolare, all'acquisizione della morfologia del volto dei passeggeri in transito presso l'aeroporto di Fiumicino. Più specificamente l'impianto ipotizzato mira a controllare e, in prospettiva, razionalizzare le code che si formano nelle varie fasi che precedono l'imbarco dei passeggeri.

Le finalità del trattamento spaziano dall'esigenza di migliorare i servizi alla clientela, all'aumento delle generali condizioni di sicurezza dello scalo, alla gestione più sicura delle delicate fasi dei controlli di sicurezza e di verifica passaporti. Al termine dell'istruttoria il Garante ha acconsentito alla realizzazione di tale sistema avendo cura tuttavia di impartire alcune prescrizioni al fine di garantire, in particolare, che il trattamento dei dati sia assistito da congrue misure di sicurezza.

Amt s.p.a.

Con provvedimento 1° marzo 2018, n. 123 (doc. web n. 8159431), il Garante ha autorizzato l'azienda mobilità e trasporti di Genova (Amt s.p.a.) ad installare sul parabrezza anteriore dei propri veicoli aziendali un dispositivo denominato *Roadscan* DTW in grado di registrare, in caso di incidenti, le immagini relative alla sede stradale prospiciente il veicolo (o, su comando attivato dall'autista, le immagini della zona interna del veicolo) e localizzare il veicolo stesso. Il trattamento è stato autorizzato per la sola finalità di ricostruzione della dinamica di eventuali sinistri e al fine di prevenire episodi illeciti a bordo dei veicoli, nel rispetto di idonee misure di sicurezza volte a preservare l'integrità dei dati e prevenire accessi abusivi da parte di soggetti non autorizzati. Il Garante ha prescritto che i dati relativi alla localizzazione tramite Gps non potranno essere utilizzati per rintracciare *online* il veicolo né per definire a posteriori i percorsi effettuati; inoltre il titolare del trattamento dovrà predisporre un modello semplificato di informativa inglobata in un pittogramma, da collocare su ogni veicolo aziendale, che renda noto agli interessati che in caso di sinistro le immagini verranno registrate.

14.7. *Trattamento di dati in ambiti particolari*

Nuovo Imaie

Con provvedimento 1° febbraio 2018, n. 54 (doc. web n. 8125264), il Garante ha esaminato l'istanza con cui il Nuovo istituto mutualistico artisti interpreti esecutori (Nuovo Imaie), soggetto formalmente accreditato nel registro delle imprese di intermediazione dei diritti connessi al diritto d'autore e che, allo stato, rappresenta oltre undicimila artisti, ha chiesto l'adozione di un provvedimento di bilanciamento di interessi, ai sensi dell'art. 24, comma 1, lett. *g*), d.lgs. n. 196/2003, ai fini della comunicazione dei dati personali degli iscritti agli altri organismi di gestione collettiva (*collecting*) di tali diritti che operano in regime di concorrenza tra loro, in mancanza del consenso degli artisti, interpreti ed esecutori medesimi.

In particolare, in ottemperanza alla deliberazione 22 marzo 2017 con cui l'Agcm ha definito l'istruttoria avviata nei confronti di Nuovo Imaie per l'accertamento di presunte condotte anticoncorrenziali poste in essere in violazione dell'art. 102 del Trattato sul funzionamento dell'Unione europea, Nuovo Imaie è tenuto a trasmettere alle altre *collecting* le informazioni contenute nella banca dati in suo possesso esclusivo, affinché queste ultime dispongano della base informativa necessaria per operare in condizione di parità competitiva, come previsto dal legislatore; ciò "nella misura in cui il trattamento risulti compatibile con la normativa in materia di protezione dei dati personali".

Il Garante quindi, dopo aver attentamente valutato la tipologia di dati personali oggetto di comunicazione, ha autorizzato tale comunicazione, indipendentemente dal consenso degli interessati, ma limitatamente ai dati essenziali al raggiungimento

14

Concorso a premi e dati sensibili

delle finalità concorrenziali, prevedendo al tempo stesso che in ragione dell'elevato numero di interessati, i *collecting* possano rendere un'informativa completa di tutti gli elementi previsti dall'art. 13 del Codice secondo modalità alternative e semplificate (attraverso ad es. la pubblicazione di un avviso sui propri siti web – o altro mezzo ritenuto idoneo – nonché mediante la comunicazione della stessa agli interessati in occasione del primo contatto).

Il Garante, con provvedimento 29 marzo 2018, n. 180 (doc. web n. 8983338), si è pronunciato relativamente ad una richiesta di autorizzazione al trattamento di dati sensibili (segnatamente, dati idonei a rivelare la vita sessuale), presentata da una società operante nel settore della distribuzione di arredamenti, concernente il trattamento di dati personali riferiti ai partecipanti ad un concorso a premi rivolto a coppie dello stesso sesso intenzionate a costituire un'unione civile. Il Garante, nell'autorizzare il suddetto trattamento in ragione delle "circostanze particolari" che caratterizzavano la richiesta (art. 41, d.lgs. n. 196/2003), ha prescritto l'adozione di idonee misure e accorgimenti a garanzia degli interessati, con particolare riferimento alle istruzioni che il titolare è tenuto a fornire ai soggetti autorizzati a trattare i dati, alla messa in atto di adeguate misure di sicurezza nonché all'esatta individuazione dei tempi di conservazione. Inoltre, è stata evidenziata la necessità di riformulare l'informativa da rilasciare agli interessati al fine di meglio evidenziare le distinte finalità perseguite dal titolare (segnatamente di "espletamento" e di "promozione" del concorso a premi), nonché il carattere facoltativo del conferimento di alcuni dati personali dei partecipanti.

14.8. *Piattaforma IMI* (Internal Market Information System)

Fin dai primi giorni di vigenza delle nuove disposizioni regolamentari sono confluiti sulla cd. piattaforma IMI molti casi riguardanti i cd. trattamenti transfrontalieri di dati.

IMI è una piattaforma multilingue che consente un veloce e sicuro scambio di comunicazioni fra autorità pubbliche interessate dalla corretta applicazione del diritto dell'Unione. Il sistema è stato sviluppato dalla Commissione europea in stretta collaborazione con i Paesi membri ed è operativo dal 2008.

La piattaforma consente alle autorità pubbliche interessate di adempiere ai propri obblighi di cooperazione amministrativa transfrontaliera e attualmente supporta 12 settori legali di interesse con 34 diverse procedure strutturate. Le autorità pubbliche registrate sono oltre 7.800 con più di 1.500 scambi al mese.

Data la flessibilità che ne consente l'adattabilità a nuovi settori di interesse, la piattaforma IMI è stata scelta per supportare i meccanismi di cooperazione e coerenza previsti dal RGPD. La sezione dedicata a quest'ultimo è pertanto il 13° settore di interesse supportato da IMI. Nel complesso lavoro di adattamento della piattaforma alle nuove esigenze, la Commissione (in particolare la DG Grow) ha lavorato in stretto contatto con il Segretariato del Comitato europeo per la protezione dei dati (EDPB-*European Data Protection Board*). Le autorità di controllo dei 28 Paesi membri dell'Unione europea, nonché dei tre Paesi facenti parte dell'EEA (Spazio economico europeo) rappresentati nell'ambito di una *task force* (*Future users group*) riunitasi a Bruxelles tra dicembre 2017 e marzo 2018 hanno quindi formulato le proprie osservazioni contribuendo a delineare l'attuale architettura della piattaforma ed a validare il contenuto e le caratteristiche dei diversi moduli e procedure previste dal sistema.

Dal 25 maggio 2018, la sezione RGPD della piattaforma IMI è operativa e viene utilizzata da tutte le autorità di controllo per cooperare tra loro al fine di garantire

una coerente tutela dei dati personali all'interno dell'Unione europea. Inoltre, nella seduta plenaria del 24-25 settembre 2018 il Comitato europeo per la protezione dei dati ha assegnato all'EDPB IMI *help desk* una funzione non solo di supporto tecnico ma anche di complessivo monitoraggio del sistema allo scopo di assistere le autorità nel corretto utilizzo della piattaforma. Attraverso IMI le autorità possono ora contare su uno strumento trasparente, flessibile e sicuro per diverse finalità, quali, ad esempio, identificare l'autorità capofila nel caso di trattamenti transfrontalieri e successivamente contribuire all'elaborazione di un progetto di decisione condiviso fra l'autorità capofila e le autorità interessate (cd. meccanismo dello sportello unico o *one stop shop*) oppure assicurare assistenza reciproca attraverso lo scambio di informazioni o condurre indagini e misure di contrasto congiunte. Infine, allo scopo di favorire un'applicazione coerente del RGPD in tutta l'Unione, è previsto che la piattaforma venga utilizzata altresì per consentire alle autorità di controllo di consultare il Comitato europeo per la protezione dei dati al fine di raccoglierne un parere, ad esempio per questioni di applicazione generale o che producono effetti in più di un Paese membro o anche per ottenere una decisione vincolante del Comitato che componga eventuali conflitti fra le stesse autorità di controllo.

Per quanto concerne il merito dei casi pervenuti al Garante dal 25 maggio in poi va rilevato che gli stessi riguardano casistiche eterogenee e sono riferiti ad una variegata pluralità di titolari del trattamento, richiedendo ai dipartimenti interessati una complessa attività istruttoria al fine di individuare in primo luogo la rilevanza transfrontaliera del caso, attività che risulta ancora più gravosa considerato che nella maggioranza dei casi, in questa prima fase di funzionamento, i documenti "caricati" sulla piattaforma sono allegati nella lingua originale e non tradotti in inglese, come invece previsto, mentre in altre ipotesi le informazioni riguardanti talune fattispecie sono risultate piuttosto scarne o sprovviste di idonea documentazione. Inoltre, alcune criticità sono emerse laddove, una volta accertata la rilevanza transfrontaliera, è risultato che la fattispecie considerata, avendo un impatto esclusivamente "locale", avrebbe dovuto essere trattata dall'autorità nazionale interessata mediante la procedura a ciò specificamente prevista in IMI che richiede l'esclusiva partecipazione dell'autorità capofila senza il necessario coinvolgimento delle altre autorità di controllo.

In ogni caso, all'esito dell'esame di questa prima fase di funzionamento, emerge come le autorità di controllo stiano utilizzando la piattaforma IMI assai attivamente. Basti pensare che dal 25 maggio 2018 per il solo profilo concernente l'identificazione dell'autorità capofila sono già centinaia le procedure attivate.

14.9. *Accreditamento e certificazioni*

Il Garante ha continuato la collaborazione con le altre autorità europee per la protezione dei dati in ordine all'istituzione di meccanismi per la certificazione della protezione dei dati personali. I lavori hanno riguardato in particolare la stesura dei documenti concernenti, rispettivamente, l'identificazione di criteri comuni per accreditare gli organismi di certificazione e i requisiti aggiuntivi per l'accreditamento, ai sensi dell'art. 43, par. 1, lett. *b*), del RGPD, e quelli aventi ad oggetto l'identificazione di criteri comuni per la certificazione dei trattamenti, che hanno portato all'elaborazione delle *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) e delle Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.*

A livello nazionale sono proseguiti gli approfondimenti sul tema nell'ambito del tavolo di lavoro istituito con Accredia nel 2017 per garantire l'avvio delle attività di accreditamento e certificazione nel rispetto del RGPD e acquisire elementi utili all'individuazione dei requisiti aggiuntivi per l'accreditamento, ai sensi dell'art. 43, par. 3, e dei criteri di certificazione in base all'art. 42, par. 5, del RGPD. All'esito di tale collaborazione è stata sottoscritta la convenzione volta a favorire lo scambio di informazioni in merito alle attività di accreditamento, nonché a valorizzare le reciproche competenze (cfr. doc. web n. 9099622); potranno così essere accreditati gli organismi di certificazione e, di conseguenza, certificate le organizzazioni che ne facciano richiesta.

Sempre nell'anno di riferimento, di particolare rilievo è stata la scelta effettuata dal legislatore nazionale con il decreto legislativo n. 101/2018 che ha individuato in Accredia, in quanto Ente unico nazionale di accreditamento, istituito ai sensi del regolamento (CE) n. 765/2008, l'organismo nazionale di accreditamento deputato all'accreditamento degli organismi di certificazione secondo quanto previsto nell'art. 43, par. 1, lett. *b*), del RGPD (cfr. in particolare art. 2-*septiesdecies*, d.lgs. n. 101/2018).

L'art. 43, infatti, prevede che gli Stati membri garantiscano che gli organismi di certificazione siano accreditati dall'autorità di controllo competente ai sensi degli artt. 55 o 56 e/o dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008. Merita evidenziare che il legislatore nell'effettuare tale scelta ha comunque riservato al Garante il potere di assumere direttamente l'esercizio di tali funzioni, mediante deliberazione pubblicata nella Gazzetta ufficiale, con riguardo a particolari categorie di trattamenti o qualora l'Ente unico nazionale di accreditamento non assolva ai suoi compiti.

15 Violazione di dati personali *(data breach)*

15.1. *I controlli: il caso Uber*

Nel corso del 2018 il Garante ha svolto un'intesa attività di collaborazione con alcune autorità di protezione dei dati europee nell'ambito della *task force* (composta anche da rappresentanti delle autorità francese, spagnola, belga, tedesca e britannica e coordinata dall'Autorità garante olandese) istituita per indagare su una violazione di dati personali (*data breach*) che ha coinvolto i dati di decine di milioni di interessati in tutto il mondo. La violazione subìta a seguito di un attacco *hacker* verificatosi nel 2016, ma resa pubblica soltanto nel mese di novembre del 2017, ha riguardato il gruppo multinazionale Uber (la cui capogruppo Uber technologies inc. ha sede negli Stati Uniti); gruppo che fornisce un servizio di trasporto automobilistico privato attraverso un'applicazione mobile (cd. *app*) volta a mettere in collegamento diretto passeggeri e autisti, e ha interessato, per lo più, dati identificativi e di contatto, informazioni concernenti la localizzazione, l'*account* e, con specifico riferimento agli autisti, anche il numero della patente di guida. Scopo principale della suddetta *task force* è stata la condivisione delle posizioni assunte dalle autorità interessate nell'ambito delle istruttorie condotte a livello nazionale.

Già alla fine del 2017 il Garante ha infatti tempestivamente avviato alcuni accertamenti – anche mediante ispezioni effettuate *in loco* presso la sede della società del gruppo stabilita in Italia – al fine di acquisire maggiori elementi di valutazione in ordine alla portata in ambito nazionale di tale incidente di sicurezza che ha visto coinvolti i dati personali di circa 295 mila utenti italiani (tra passeggeri e autisti).

Tenuto conto delle risultanze istruttorie e della documentazione acquisita nonché del relativo quadro normativo di riferimento, sono stati accertati vari profili di non conformità riguardo al trattamento dei dati di utenti presenti nel nostro Paese. Innanzitutto in ordine all'ambito soggettivo, la rappresentazione dei ruoli fornita dal gruppo Uber in termini di titolarità esclusiva in capo ad Uber B.V. (società, con sede nei Paesi Bassi, avente la responsabilità della raccolta e del trattamento dei dati personali degli utenti sul territorio europeo) per i dati relativi ad "utenti che risiedono al di fuori degli Stati Uniti" non è apparsa coerente con quanto riscontrato in sede di accertamento e ha reso necessario configurare piuttosto in termini di contitolarità del trattamento il rapporto esistente tra Uber Technologies Inc. e Uber B.V. Al riguardo, infatti, oltre ad essere stata accertata l'esistenza di un unico *database* centralizzato situato negli Stati Uniti, si è anche potuto constatare che la società capogruppo predispone le *policy* di funzionamento e di gestione del servizio anche in ordine alle misure di sicurezza, concependole in maniera unitaria nell'interesse di tutte le società del gruppo, residuando di fatto in capo ad Uber B.V. solo alcuni poteri decisionali per lo più limitati ad attività di mero "adattamento" al contesto locale. La riqualificazione di tale rapporto ha comportato immediate ripercussioni sulla conformità alla normativa di protezione dei dati dell'informativa rilasciata agli utenti da Uber, e per tali ragioni si è ritenuto che la stessa non sia stata formulata correttamente, oltre ad essere risultata incompleta e poco chiara. In particolare, si è evidenziato che non erano sufficientemente specificate le finalità del trattamento in relazione alla molteplicità di categorie di dati personali raccolti, i riferimenti ai

diritti dell'interessato apparivano generici e lacunosi e non era neppure chiaro se gli utenti fossero obbligati o meno a fornire alcuni dati personali, né quali fossero le conseguenze in caso di diniego. Il Garante ha poi rilevato che Uber ha trattato i dati dei passeggeri ai fini dell'individuazione di un "indice di rischio frode" senza che gli interessati siano stati adeguatamente informati al riguardo e abbiano reso un valido consenso in tal senso. Infine è stato constatato che la società non ha adempiuto all'obbligo di notificare all'Autorità il trattamento dei dati per finalità di geolocalizzazione, così come previsto dalla normativa in vigore prima del RGPD (art. 37, comma 1, lett. *a*), d.lgs. n. 196/2003). Alla luce di tali esiti, il Garante si è dunque pronunciato con il provvedimento 13 dicembre 2018, n. 498 (doc. web n. 9069046), facendo al contempo presente che avvierà un autonomo procedimento per contestare le violazioni amministrative così accertate anche in considerazione di quanto disposto dall'art. 164-*bis*, comma 2, d.lgs. n. 196/2003.

15.2. *Gestione delle notifiche di violazione di dati personali*

Nei primi mesi del 2018 il Garante, in vista delle modifiche introdotte dall'art. 33 del RGPD alla disciplina relativa alla violazione di dati personali – vale a dire la "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" (art. 4, punto 12, del RGPD) –, ha provveduto a riorganizzare la gestione delle notifiche delle violazioni affidandone la trattazione al Dipartimento tecnologie digitali e sicurezza informatica che, a partire da marzo 2018, ha curato le relative istruttorie, per i profili di carattere tecnologico, in coordinamento con i dipartimenti competenti per i profili di carattere giuridico.

In tali attività istruttorie compito prioritario è stato quello di individuare prontamente, collaborando con i titolari dei trattamenti coinvolti nelle violazioni dei dati, le misure da adottare idonee a mitigarne gli effetti negativi, valutando altresì l'opportunità della comunicazione della violazione agli interessati una volta stimata l'entità del rischio per i diritti e le libertà delle persone fisiche.

L'Ufficio ha acquisito gli elementi necessari alla valutazione della gravità delle violazioni oggetto di notifica sia attraverso acquisizione documentale sia attraverso specifiche attività ispettive presso i titolari e i responsabili del trattamento. Nei casi di mancata notificazione della violazione, comunque pervenuta a conoscenza dell'Autorità tramite altri canali (ad es., notizie di stampa o segnalazioni di interessati), l'istruttoria è stata avviata d'ufficio.

Dal 1° marzo al 31 dicembre 2018 sono pervenute all'Autorità 650 notifiche di *data breach* – di cui 630 dal 25 maggio al 31 dicembre 2018, che hanno riguardato, come titolari del trattamento, soggetti pubblici (27% dei casi) e soggetti privati (73% dei casi).

Le tipologie di violazione più frequenti hanno riguardato:

– attacchi informatici volti all'acquisizione di dati personali (quali, credenziali di accesso, indirizzi e-mail, numeri di telefono o dati relativi a strumenti di pagamento);

– diffusione di virus di tipo *ransomware*;

– smarrimento o furto di dispositivi digitali o documenti cartacei;

– comunicazione o diffusione accidentale di dati personali.

16 Il trattamento di dati personali nell'ambito del condominio

In materia di condominio l'attività dell'Autorità è stata prevalentemente indirizzata a fornire, a fronte delle specifiche richieste e segnalazioni inoltrate dai cittadini, chiarimenti rispetto ai profili attinenti il tema del trattamento di dati personali anche alla luce dei principi ora sanciti dal RGPD.

In tali occasioni, l'Autorità ha colto l'occasione per confermare, in termini generali, quanto già indicato nel provvedimento 18 maggio 2006 in merito al trattamento di dati personali nell'ambito dell'amministrazione di condomini (doc. web n. 1297626); chiarendo, con particolare riguardo agli ancora frequenti casi in cui le informazioni inerenti i singoli interessati partecipanti alla compagine condominiale sono oggetto di illecita comunicazione e/o diffusione, che le informazioni relative a quest'ultimi possono essere comunicate a terzi solo con il consenso espresso degli interessati, ovvero in presenza di altri presupposti di liceità legislativamente previsti, come ora individuati nell'art. 6 del RGPD e comunque nel rispetto dei principi generali di cui all'art. 5 del medesimo Regolamento. Il Garante ha al contempo ribadito che le informazioni personali riferibili a ciascun partecipante possono essere trattate per la finalità di gestione ed amministrazione del condominio e che possono essere per tali ragioni condivise all'interno della compagine condominiale, tenendo anche conto che i condomini devono essere considerati contitolari di un medesimo trattamento dei dati (v. ora art. 4, par. 1, n. 7 e Capo IV, in particolare art. 26, del RGPD) di cui l'amministratore ha la concreta gestione e che quest'ultimo agisce in tale contesto nell'eventuale veste di responsabile del trattamento (v. ora art. 4, par. 1, n. 8 e Capo IV del RGPD).

Sono state inoltre nuovamente oggetto di attenzione da parte del Garante le disposizioni a suo tempo introdotte con la legge 11 dicembre 2012, n. 220 (recante la riforma in materia di condominio negli edifici), in particolare quella inerente il registro di anagrafe condominiale (cfr. art. 1130, comma 1, punto 6, c.c.) e quelle concernenti gli obblighi di trasparenza previsti in materia di gestione contabile del condominio. Al riguardo, l'Autorità, come rappresentato già in passato (cfr. Relazione 2015, p. 130), ha puntualizzato, a fronte di diverse quesiti in ordine alla possibilità di accesso al citato registro da parte degli interessati, che la conoscibilità delle informazioni concernenti i partecipanti alla compagine condominiale deve restare impregiudicata qualora ciò sia conforme alla disciplina civilistica o comunque sia prevista in base ad altre norme presenti nell'ordinamento, purché sussistano i relativi presupposti fissati dalla legge, e che pertanto il registro in questione può essere visionato dagli interessati nei termini indicati dall'art. 1129, comma 2 c.c. previa richiesta all'amministratore. Muovendo dallo stesso presupposto l'Autorità ha sottolineato come dall'esame delle disposizioni introdotte dalla riforma possa rilevarsi il diritto in capo ai condomini (ma anche ai titolari di un diritto reale o di godimento) di poter prendere visione in qualsiasi momento dei documenti di spesa in possesso dell'amministratore nonché di poter estrarne copia al fine di avere in ogni tempo un quadro chiaro della situazione contabile del condominio; ciò anche attraverso la consultazione del cd. registro contabile (cfr., in tal senso, artt. 1130, comma 1, n. 7, 1129, comma 2, e 1130-*bis*, comma 1, c.c.).

17 Il trasferimento di dati personali all’estero

L’attività del Garante nel settore dei trasferimenti di dati personali verso Paesi terzi si è prevalentemente incentrata sulle novità normative introdotte dal RGPD (v. Capo V), con particolare riferimento al venir meno delle autorizzazioni nazionali in materia di clausole tipo, decisioni di adeguatezza e norme vincolanti d’impresa (*Binding corporate rules* – Bcr); all’introduzione di nuovi strumenti per i trasferimenti transfrontalieri (ad es., meccanismi di certificazione, codici di condotta, accordi tra autorità pubbliche); alla previsione di specifici meccanismi di cooperazione tra autorità di protezione dei dati (art. 64 del RGPD) per l’approvazione (ad es., Bcr) o l’adozione (ad es., clausole tipo) degli stessi.

Le modifiche legislative sopra citate hanno nei fatti delimitato, a far data dal 25 maggio 2018, i casi in cui il Garante può intervenire con provvedimenti di autorizzazione a livello nazionale – ad oggi infatti circoscritti ad ipotesi specifiche per lo più caratterizzate da circostanze particolari (v. art. 46, par. 3, del RGPD) – e al contempo hanno previsto una sua maggiore partecipazione, per il tramite dei sopra indicati meccanismi di cooperazione, al procedimento di elaborazione e di approvazione delle “garanzie adeguate” previste al Capo V del RGPD.

In tale ottica, è stata pertanto dedicata particolare attenzione ai lavori del comitato per la protezione dei dati volti alla revisione dei documenti del Gruppo Art. 29 in materia di decisioni di adeguatezza, norme vincolanti d’impresa e deroghe in specifiche situazioni; al contempo, sono state intraprese diverse attività volte ad agevolare il passaggio alla nuova disciplina regolamentare nella materia dei trasferimenti di dati personali. Pertanto, oltre all’adozione, come già avvenuto in passato, di alcuni provvedimenti autorizzativi in materia di trasferimenti di dati personali verso Paesi terzi mediante Bcr (provv.ti 1° febbraio 2018, n. 51, doc. web n. 8043179; 15 febbraio 2018, n. 81, doc. web n. 8017730), l’Autorità è altresì intervenuta con il provvedimento 16 maggio 2018, n. 293 (doc. web n. 8990209) in merito ad alcune Bcr approvate a livello europeo ma prive, alla data del 24 maggio 2018, della relativa autorizzazione nazionale. In questo contesto, si è tenuto conto della circostanza che, nelle more del passaggio dalla precedente disciplina (direttiva 95/46/CE) al nuovo quadro regolamentare, le Bcr, per le quali, la procedura europea di cooperazione era giunta a conclusione, non avrebbero potuto essere considerate comunque uno strumento adeguato per i relativi trasferimenti transfrontalieri dal territorio italiano in quanto prive della relativa autorizzazione nazionale. Il Garante ha perciò autorizzato, con un provvedimento di carattere generale, tutti i trasferimenti intra-gruppo di dati personali dall’Italia verso Paesi non appartenenti all’Unione europea oggetto delle Bcr approvate a livello europeo nell’ambito delle sopra menzionate procedure entro il 24 maggio 2018, considerandoli adeguati ai sensi dell’art. 44, d.lgs. n. 196/2003. Con il medesimo provvedimento l’Autorità ha rappresentato ai gruppi di impresa destinatari del predetto provvedimento la necessità (ai sensi del WP 256 e del WP 257) di rendere le Bcr ivi individuate conformi al RGPD, notificando a tutti i membri del gruppo e alle autorità di controllo nazionali, con cadenza annuale a far data dal 25 maggio 2018, le modifiche apportate a tal fine.

18 Il Registro dei trattamenti

18.1. *La notificazione*

La notificazione, il cui obbligo, come meglio evidenziato nel paragrafo successivo, è stato soppresso nel corso del 2018, era una dichiarazione con la quale un titolare del trattamento (sia soggetto pubblico che privato) rendeva nota l'effettuazione di un determinato trattamento di dati personali (specificando una serie di informazioni obbligatorie) affinché, attraverso l'inserimento nel Registro dei trattamenti, tali informazioni venissero rese pubbliche.

Le notificazioni erano inserite in un Registro pubblico, tuttora liberamente e gratuitamente consultabile *online* tramite il sito dell'Autorità, da cui chiunque può acquisire notizie e utilizzarle per le finalità di applicazione della disciplina in materia di protezione dei dati personali (ad es., per esercitare il diritto di accesso ai dati o gli altri diritti riconosciuti dal Codice).

18.2. *Evoluzione delle notificazioni nel 2018 e soppressione dell'obbligo*

Nella prima parte del 2018 è proseguita l'attività di controllo, sia nei confronti dei titolari iscritti nel Registro sia nei confronti di quelli che effettuano trattamenti oggetto di notificazione ma che non risultano presenti nel Registro; tale attività è stata effettuata anche mediante ispezioni *in loco*, nell'ambito della programmazione ispettiva di cui si è dato conto al par. 21.2.

In particolare, dai controlli effettuati nel corso dell'anno sono emersi 17 casi di omessa o incompleta notificazione del trattamento e sono state contestate le relative violazioni ai titolari del trattamento. La maggior parte delle violazioni è stata riscontrata con riferimento al trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (art. 37, comma 1, lett. *a*), del Codice).

In tutti i casi in cui sono state riscontrate violazioni, sono stati quindi avviati i procedimenti per l'applicazione della sanzione prevista dall'art. 163 del Codice che prevede una pena pecuniaria da 20.000 a 120.000 euro.

Va segnalato, tuttavia, che nella seconda parte dell'anno tale attività è stata interrotta; infatti, in conformità a quanto previsto dal RGPD, il d.lgs. n. 101/2018 (art. 22, comma 8) ha stabilito che il Registro dei trattamenti di cui all'art. 37, comma 4, del Codice, cessasse di essere alimentato a far data dal 25 maggio 2018.

Il citato decreto legislativo n. 101/2018 ha altresì stabilito che, fino al 31 dicembre 2019, il Registro resterà accessibile a chiunque secondo le modalità già previste dal Codice, ovvero attraverso il sito web del Garante all'indirizzo https://web.garanteprivacy.it/rgt/NotificaTelematica.php.

In tale quadro è stato predisposto uno specifico avviso, pubblicato sul sito del Garante, al fine di chiarire i termini di cessazione dell'obbligo e la permanente possibilità di accesso al Registro. Ciononostante, dopo il 25 maggio, ed in particolare nei primi mesi del secondo semestre 2018, hanno continuato a pervenire numerose richieste telefoniche di chiarimento circa la cessazione dell'obbligo e l'accesso al

Registro (circa 150) nonché richieste di credenziali utili alla notificazione, di attestazione di pagamento e di rimborso (circa 50).

Complessivamente, nel periodo di previsione dell'obbligo di notificazione, cioè dal 1° gennaio 2004 al 24 maggio 2018, come meglio specificato nella sezione relativa ai dati statistici, sono affluite nel Registro n. 33.019 notificazioni. In relazione alle somme incassate per le notificazioni effettuate dai titolari del trattamento, si evidenzia che nel periodo di previsione dell'obbligo, sopra specificato, sono stati complessivamente incassati € 4.952.850, per una media annua di € 330.190 (cfr. tab. 11-13).

19 La trattazione dei ricorsi

19.1. *Considerazioni generali*

La relazione sull'attività dei ricorsi per l'anno 2018 – che riguarda, in realtà, solo il primo semestre dell'anno di riferimento – racchiude gli esiti di un lavoro strutturato nell'arco di vent'anni che, complice anche la specificità dello strumento previsto, è riuscito a mantenere nel tempo una propria caratterizzazione di fondo che ha contraddistinto questo settore dagli altri ambiti di intervento nei quali si è concretizzato l'impegno dell'Autorità.

Il cambiamento dello scenario normativo di cui la disciplina della protezione dei dati è stata protagonista negli ultimi anni, culminato nell'adozione del RGPD, ha avuto inevitabili ricadute anche sulla disciplina dei ricorsi che, come già evidenziato nella Relazione 2017, ha ceduto il passo ad uno strumento di tipo diverso, ovvero il reclamo di cui all'art. 77 del RGPD.

Si è trattato, a dire il vero, di una scelta non inevitabile tenuto conto del fatto che la formulazione dell'art. 77, par. 1, del RGPD avrebbe, in astratto, consentito di fare salvi meccanismi di tutela che, pur disciplinati dalla normativa nazionale, non risultassero incompatibili con il disegno complessivamente desumibile dalla lettura del testo normativo europeo. In questo senso il ricorso agli artt. 145 ss., d.lgs. n. 196/2003 avrebbe potuto, in virtù della sua specifica snellezza procedimentale nonché delle particolari garanzie riconosciute alle parti, integrare i requisiti minimi di tutela cui il RGPD vincola gli Stati membri nella definizione dell'*iter* procedimentale attivato a seguito dell'*input* fornito dal reclamante.

Ma proprio la specificità del procedimento dettato dalla normativa nazionale, costituendo un *unicum*, ha portato a ritenere preferibile l'utilizzo di uno strumento diverso che consentisse, da un lato, di creare una base comune in ambito europeo, quanto meno nella fase della sua attivazione, e dall'altro di uniformare le modalità di trattazione delle istanze degli interessati senza differenziare le ipotesi di esercizio esclusivo dei diritti da quelle aventi ad oggetto indagini più ampie sul trattamento di dati complessivamente inteso. Del resto, nell'esperienza dei ricorsi, è spesso accaduto che la decisione sul singolo diritto esercitato dall'interessato abbia richiesto una verifica da parte dell'Autorità in ordine alla liceità del trattamento svolto dal titolare (come, ad es., nelle ipotesi di richiesta di cancellazione di cui all'art. 7, comma 3, lett. *b*), d.lgs. n. 196/2003), tale da implicare un accertamento più esteso che, tuttavia, per le caratteristiche intrinseche del procedimento, non poteva che essere reso in via incidentale nei limiti di quanto funzionale alla decisione da adottare nel caso concreto.

Lo strumento del reclamo, consentirà, presumibilmente, di uscire dal sentiero tradizionale battuto finora, aprendo la via, in molte ipotesi, ad una valutazione più ampia sul trattamento posto in essere dal titolare idonea, come tale, ad integrare i presupposti dello svolgimento della funzione di controllo che fa da contraltare al principio di *accountability*. Per fare ciò occorre, tuttavia, tener fede ad alcuni requisiti procedurali minimi richiesti dal RGPD al fine di garantire, pur nell'ottica della semplificazione delle forme e dei tempi di definizione dei reclami, un esercizio imparziale ed equo dei poteri affidati alle autorità di protezioni dei dati.

In quest'ottica è auspicabile che si possa comunque attingere, in una sorta di continuità con il passato, dalla cospicua esperienza maturata in modo da rendere più agevole, nella gestione dei casi concreti, l'adeguamento alle nuove disposizioni.

19.2. *Dati statistici*

I ricorsi decisi nel primo semestre del 2018 sono stati pari a 130, numero che sembrerebbe confermare un certo assestamento nell'uso dello strumento previsto dal Codice (cfr. sez. IV, tab. 4 e 5). Tuttavia a questo dato sono da aggiungere gli atti la cui istruttoria è stata avviata, ma non conclusa alla data del 25 maggio 2018 (pari a 5), nonché quelli, pari a 34, che, essendo pervenuti a ridosso di tale data, non sono stati gestiti secondo il rito procedimentale dei ricorsi, ormai prossimo alla cessazione, ma trattati sulla base di disposizioni diverse. Sulla base di queste informazioni si può pertanto ragionevolmente ritenere che, se l'arco temporale preso a riferimento fosse stato l'intero anno, il numero complessivo dei ricorsi avrebbe molto probabilmente avuto, in confronto con gli anni passati, un sensibile aumento.

Del resto il moto oscillatorio che, nel corso dei vent'anni trascorsi, ha caratterizzato l'utilizzo di questo mezzo di tutela – sia con riguardo al numero complessivo (basti constatare la crescita esponenziale avuta sino al 2004 ed il successivo, tendenziale, decremento che ha toccato la punta minima nel 2013 con 222 decisioni), che con riferimento alla distribuzione dei ricorsi nelle varie aree tematiche – ha fornito importanti indizi non solo in ordine alla sua efficacia, ma anche con riguardo alla tipologia di interessi che, nei vari periodi, sono stati percepiti dalla collettività come maggiormente meritevoli di protezione, dando in tal modo impulso all'attività dell'Autorità anche tramite interventi di altro tipo (come, ad es., provvedimenti di carattere generale, codici di deontologia e buona condotta, ecc.).

In quest'ottica, i dati statistici del 2018 evidenziano, in continuità con quanto già emerso negli anni precedenti ed in particolare a partire dal 2015, la netta preminenza dei ricorsi collegati al settore dell'editoria (39%), da intendersi come comprensivo anche di quelli presentati nei confronti dei gestori dei motori di ricerca che, in termini relativi, costituiscono la maggioranza delle richieste, confermando la grande attenzione rivolta dal pubblico agli effetti pregiudizievoli connessi alla diffusione in rete di dati personali.

Il nuovo approccio al tema determinato dagli effetti prodotti dalla sentenza della CGUE 13 maggio 2014 C-131/12 (sentenza Google Spain) si è tradotto, in breve tempo, nella formazione di una cospicua giurisprudenza dell'Autorità con riguardo a queste fattispecie che ha peraltro favorito, al ricorrere di presupposti analoghi a quelli già positivamente valutati in sede di decisione favorevole all'interessato, un progressivo adeguamento spontaneo da parte dei titolari del trattamento.

La significativa percentuale di casi di risoluzione "amichevole" delle vicende poste all'attenzione dell'Autorità evidenzia, in modo speculare, la circostanza per la quale le decisioni di accoglimento, anche parziale, adottate nel semestre, sono invece intervenute a definire fattispecie che presentavano aspetti peculiari, tali da richiedere, pure da parte degli stessi titolari del trattamento, una specifica valutazione da parte del Garante (cfr. par. 19.4).

Una porzione dei casi trattati in questo settore ha comunque riguardato interventi di tipo più "tradizionale", legati a richieste rivolte ai titolari dei "siti-fonte" sui quali sono stati originariamente pubblicati gli articoli e dirette ad ottenere la disabilitazione della reperibilità degli stessi tramite motori di ricerca esterni a detti siti. La tematica della diffusione di dati personali tramite internet, in una visione

retrospettiva, ha sollecitato l'intervento dell'Autorità in modo consistente fin dal 2008 ove, limitatamente ad una dimensione più squisitamente nazionale, è stato affrontato il tema mediante l'elaborazione di una soluzione volta a garantire un effettivo bilanciamento dei diversi interessi in gioco – in particolare quello legato ad una dimensione prettamente individuale con il diverso diritto della collettività ad essere informata rispetto a fatti di interesse pubblico o, comunque, a poter disporre delle relative informazioni anche a scopo storico/documentaristico – imponendo agli editori, di volta in volta coinvolti, l'adozione di misure tecniche idonee ad inibire l'indicizzazione esterna degli articoli oggetto di ricorso. In molti dei casi sottoposti alla valutazione del Garante nel corso del primo semestre si è ritenuto, per lo più, di non accogliere le richieste di deindicizzazione degli articoli, ritenendo esistente, sulla base del breve lasso di tempo trascorso dai fatti, nonché delle caratteristiche specifiche delle vicende trattate, un perdurante interesse pubblico alla conoscibilità delle notizie oggetto degli articoli contestati (provv. 1° febbraio 2018, n. 63, doc. web n. 8366193; provv. 28 giugno 2018, n. 401, doc. web n. 9037315).

Rivolgendo lo sguardo a quanto avvenuto successivamente, le richieste di rimozione di risultati reperibili a partire dal nome dell'interessato rivolte ai gestori dei motori di ricerca, cresciute esponenzialmente dal 2015, hanno rappresentato la via alternativa per ottenere un risultato analogo a quello sopra descritto, anche se chiaramente con un impatto diverso.

I ricorsi in ambito economico-finanziario hanno invece costituito circa il 18% del totale (e precisamente, 11% banche e società finanziarie, 5% società di informazione commerciale e 2% società di informazioni creditizie), evidenziando una progressiva riduzione che, iniziata nel 2015, si è consolidata a partire dal 2017 (con un numero di casi analogo, in proporzione al semestre di riferimento, a quello del 2018), decretando un'inversione di tendenza rispetto al passato a vantaggio della trattazione di questioni più decisamente connesse alle problematiche legate all'utilizzo della rete e delle nuove tecnologie.

Anche in quest'area gli esiti procedimentali hanno certificato un'ampia percentuale di adesioni spontanee da parte dei titolari del trattamento, principalmente banche ed istituti di credito ai quali è stata, per lo più, avanzata richiesta di accesso ai dati riferiti a rapporti di conto corrente, in alcuni casi intestati a soggetti defunti. L'utilizzo dello strumento del ricorso non si è quindi distanziato dal solco tradizionale ormai consolidato, salvo che per profili specifici emersi, in alcuni casi, con riguardo a singole fattispecie: si pensi alle modalità prescelte dal titolare del trattamento per fornire riscontro all'interessato, fornendo parte della documentazione richiesta in formato cartaceo e parte in formato digitale scaricabile tramite il profilo utente utilizzato per accedere alla funzione di Internet banking (provv. 15 marzo 2018, n. 166, doc. web n. 8991503) oppure alla richiesta di conoscere le modalità di trattamento di dati del ricorrente utilizzati ai fini dell'invio di bollettini di pagamento di rate di finanziamento che il medesimo assumeva aver trovato apposti sul tergicristallo della propria automobile e di altre vetture posteggiate nei pressi della sua abitazione, circostanza che non ha potuto formare oggetto di valutazione da parte dell'Autorità collocandosi al di fuori dell'ambito di applicazione della normativa in materia (provv. 15 febbraio 2018, n. 94, doc. web n. 8237500).

Altro settore rilevante – pur se con una leggera flessione rispetto al 2017 – è quello legato ai rapporti di lavoro, intercorrenti con titolari pubblici e privati, che hanno confermato, con una percentuale pari al 9% del totale, una casistica varia atta a coprire dalle richieste di tipo "ordinario", connesse all'accesso al fascicolo perso-

nale, a quelle dirette a contestare l'acquisizione illecita di dati del lavoratore da parte del datore di lavoro mediante l'utilizzo indebito degli strumenti elettronici di lavoro. L'esercizio del diritto di accesso, nell'ambito di rapporti spesso conflittuali tra le parti, è stato spesso impiegato come strumento per attivare in altro ambito, in particolare giudiziario, pretese di tipo diverso, dall'impugnazione di licenziamenti reputati illegittimi (provv. 22 febbraio 2018, n. 112, doc. web n. 8458201), alla richiesta di prestazioni di carattere assistenziale da parte di enti pubblici statali (provv. 22 maggio 2018, n. 351, doc. web n. 9009344).

La restante parte dei ricorsi pervenuti può essere equamente suddivisa all'interno delle altre aree tematiche, pur non raggiungendo nel periodo di riferimento percentuali particolarmente significative, se singolarmente considerate, recuperando semmai rilievo con riguardo alle questioni trattate in fase di decisione del singolo caso (cfr. sez. IV. tab. 5). In particolare si può individuare l'area dei trattamenti posti in essere da soggetti pubblici (pari al 6%), cui vanno aggiunti quelle connessi al settore della sanità (1%, che racchiude comunque anche i trattamenti effettuati da strutture private); i trattamenti legati all'attività delle compagnie di assicurazione (che hanno raggiunto il 4% del totale dei ricorsi) e che hanno per lo più riguardato, conformemente al passato, le richieste di accesso a dati contenuti nelle relative polizze o nelle perizie medico-legali; i trattamenti a fini di marketing posti in essere da imprenditori privati (pari al 4%), nonché i trattamenti, più in generale, svolti dai fornitori telefonici e telematici (costituente il 5% del numero complessivo), nell'ambito dei quali rientrano fattispecie eterogenee (da questioni tipicamente legate all'esecuzione del rapporto contrattuale alla richiesta di accesso ai dati, ivi inclusi, con riguardo agli operatori telefonici, quelli relativi al traffico telefonico a fini di difensivi (provv. 28 giugno 2018, n. 407, doc. web n. 9038582), nonché a fini di contestazione della fatturazione (provv. 8 febbraio 2018, n. 74, doc. web n. 8256070).

19.3. *Aspetti procedurali*

Con riferimento ai profili procedurali, si è riscontrata una certa stabilizzazione relativamente ad aspetti tipicamente legati al rispetto dei requisiti formali ai quali il Codice collegava la corretta presentazione del ricorso o la sua eventuale, successiva regolarizzazione.

Questo dato risulta coerente con le decisioni di inammissibilità relative al periodo preso a riferimento (pari al 18% del totale) nell'ambito delle quali la parte più consistente ha riguardato i casi di inammissibilità diretta, ovvero quelle ipotesi nelle quali l'inammissibilità è stata dichiarata, non per assenza di requisiti formali, ma per manifesta inapplicabilità della normativa in materia di protezione dei dati personali dai casi di richiesta avanzata da persona giuridica o soggetto assimilabile – come tale esclusa dalla disciplina in materia di protezione dati per effetto di quanto è stato previsto dall'art. 40, d.l. 6 dicembre 2011, n. 201, convertito in legge 22 dicembre 2011, n. 214, scelta confermata anche dal RGPD – a quelli nei quali la domanda risultava strumentalmente formulata in modo tale da non consentire all'Autorità di effettuare una corretta valutazione della stessa (provv. 21 marzo 2018, n. 176, doc. web n. 8991523).

A queste fattispecie va aggiunta quella, nuova rispetto al passato, determinata da una sovrapposizione tra la disciplina applicabile fino al 25 maggio 2018 e le categorie giuridiche previste, da un punto di vista sostanziale, dalle norme del RGPD anticipatamente invocate dall'interessato a fondamento delle proprie pretese (provv. 15

febbraio 2018, n. 97, doc. web n. 8187745, ove si è fatto richiamo, nell'esercizio del diritto di cancellazione, all'art. 17 del RGPD).

Il mutamento delle coordinate di riferimento ha richiesto all'Ufficio, in termini procedurali, uno sforzo aggiuntivo in quanto, in assenza di indicazioni tempestive da parte del legislatore nazionale, è stato necessario individuare in modo autonomo le modalità più corrette per gestire la fase di transizione, con particolare riguardo alle istruttorie già aperte alla data del 25 maggio 2018. La fine della legislatura e l'elezione delle nuove Camere non ha infatti permesso di disporre dei tempi tecnici necessari a consentire l'esame, da parte delle Commissioni parlamentari competenti, dello schema di decreto legislativo contenente l'adeguamento della normativa nazionale alle disposizioni del RGPD – elaborato da una Commissione di esperti appositamente nominata ed approvato dal Consiglio dei ministri nella seduta del 21 marzo 2018 (cfr. par. 2.1.1) – imponendo, perciò, il ricorso alla proroga della delega per un ulteriore periodo di tre mesi che ha, infine, portato all'approvazione del decreto legislativo n. 101/2018 (sul quale v. le considerazioni svolte al punto 2.1.1).

L'Autorità ha dovuto, pertanto, far fronte alla situazione assumendo su di sé l'onere di formalizzare una scelta desumibile dall'interpretazione del quadro normativo esistente. Ciò è avvenuto mediante l'adozione di una specifica delibera (provv. 31 maggio 2018, n. 374, doc. web n. 8997237) con la quale, dichiarando l'incompatibilità sopravvenuta tra le disposizioni del Codice relative alla disciplina dei ricorsi e le nuove norme contenute nel RGPD (cfr. artt. 77 ss.), si è stabilito di disapplicare le prime, definendo, previa comunicazione agli interessati, le istruttorie non ancora concluse alla data del 25 maggio 2018 in attuazione della diversa disciplina dei procedimenti su reclamo contenuta nel Regolamento dell'Autorità n. 1/2007 (cfr. provv. 14 dicembre 2007, n. 65, doc. web n. 1477480).

Le procedure ancora aperte a quella data erano 14, delle quali 9 sono state definite nel mese di giugno 2018, dando conto, all'interno dei singoli provvedimenti, delle ragioni poste a fondamento del mutamento di rito. A questo dato deve essere aggiunto quello relativo ai 34 atti presentati in prossimità della data del 25 maggio e rispetto ai quali si è ritenuto opportuno lasciare facoltà di scelta all'interessato in ordine all'eventuale volontà di trasformare l'istanza presentata come reclamo da trattare, *ab initio*, come tale (provv. 28 giugno 2018, n. 402, doc. web n. 9037323).

Al di là delle peculiarità sopra evidenziate, legate alle contingenze del periodo, l'esperienza maturata nel corso degli anni nei quali ha trovato applicazione la disciplina dei ricorsi ha arricchito il percorso dell'Autorità di prassi e di valutazioni che costituiranno sicuramente un'utile eredità per il futuro. Il RGPD, infatti, pur apparendo orientato verso forme semplificate di approccio alla tutela invocata dall'interessato, è comunque molto rigoroso nell'invocare il rispetto, da parte degli Stati membri, di garanzie procedurali minime atte a garantire il principio del contraddittorio e l'esercizio del diritto di difesa, da sempre capisaldi della disciplina dei ricorsi (in parte, peraltro, mutuato dallo stesso Regolamento n. 1/2007 relativo ai reclami).

Ciò vale anche con riguardo ai principi desumibili dalle numerose decisioni assunte dal Garante in questi anni che possono sicuramente costituire una solida base di partenza nella gestione dei nuovi casi che saranno posti alla sua attenzione, ma che, in materia di esercizio dei diritti, ricalcano essenzialmente quanto già esistente, salvo alcuni aggiustamenti in termini ampliativi (v., ad es., il nuovo diritto di cancellazione di cui all'art. 17 del RGPD che riconosce formalmente anche il diritto all'oblio, di derivazione giurisprudenziale), nonché alcuni diritti di nuova

introduzione, quale il diritto di portabilità dei dati sul quale, salvo alcuni margini di sovrapposizione con il diritto di accesso, occorrerà compiere un'autonoma riflessione.

19.4. *I casi più significativi*

Coerentemente con la fotografia emergente nella parte della relazione dedicata alle considerazioni generali, la casistica maggiormente significativa del periodo è quella riguardante le decisioni su ricorso attestate sulla richiesta, rivolta ai gestori dei motori di ricerca, di rimuovere l'associazione presente in rete tra determinati risultati, individuati mediante specifica indicazione degli Url corrispondenti ai contenuti contestati, ed il nominativo dell'interessato.

Trattamenti di dati personali e motori di ricerca

In alcune ipotesi lo strumento del ricorso è stato utilizzato al fine di ottenere tutela con riguardo a diritti, quale quello alla reputazione, che tendenzialmente si collocano al di fuori dell'ambito di competenza dell'Autorità. Tuttavia, in molti casi, oltre all'oggettiva difficoltà di separare chirurgicamente profili tra loro strettamente collegati, si è posto il problema di rendere concreta la tutela offerta dal Codice, accogliendo il ricorso laddove l'istanza al Garante, in considerazione dell'irreperibilità del titolare del trattamento, costituiva l'unica possibilità data all'interessato per ottenere soddisfazione. È quanto avvenuto nel caso di un ricorso diretto ad ottenere la rimozione di alcuni Url da parte di un soggetto che lamentava il danno derivante alla sua reputazione professionale dalla presenza in rete di commenti diffamatori pubblicati su un *blog*, successivamente chiuso a seguito dell'intervenuta condanna per diffamazione del suo autore che, all'atto della proposizione dello stesso, non risultava rintracciabile. Il Garante, considerato il significativo lasso di tempo trascorso rispetto agli eventi, collocabili tra il 2006 ed il 2011, che valeva ad attenuare sensibilmente l'interesse pubblico alla reperibilità delle informazioni, ha ritenuto fondato il ricorso, tenuto peraltro conto del fatto che, l'irreperibilità dell'autore del *blog*, rendeva la deindicizzazione degli Url indicati l'unica misura idonea a contenere gli effetti potenzialmente pregiudizievoli della diffusione dei commenti pubblicati (provv. 25 gennaio 2018, n. 36, doc. web n. 8342396).

Fattispecie analoga, anche se con profili in parte diversi, è stata quella relativa alla richiesta di rimozione di un Url collegato ad un *post* pubblicato da un soggetto non identificabile all'interno di una piattaforma informatica – gestita dalla società titolare del motore di ricerca avverso il quale è stato proposto ricorso – e contenente un commento lesivo consistente nell'attribuzione all'interessato di reati ai quali lo stesso si è invece dichiarato estraneo, producendo idonea documentazione atta a comprovare quanto affermato. Il Garante, a fronte della specifica eccezione sollevata dal titolare del trattamento, ha preliminarmente affermato l'ammissibilità della richiesta in quanto concretamente diretta ad ottenere la rimozione dell'Url che conduceva al commento piuttosto che del contenuto di quest'ultimo, decidendo poi, nel merito, per l'accoglimento di essa, rilevando che il gestore di un motore di ricerca deve comunque assicurare un trattamento conforme ai principi vigenti in materia di protezione dei dati personali – tra i quali quello di esattezza del dato – e valorizzando altresì, come nel caso precedentemente esposto, la circostanza che il ricorso costituiva, nel caso di specie, l'unico strumento a disposizione del ricorrente per arginare la diffusione del contenuto lesivo (provv. 1° febbraio 2018, n. 65, doc. web n. 8384511).

Nell'ambito dello stesso filone può citarsi il caso di richiesta di rimozione di Url che, pur risultando associati al nominativo del ricorrente, erano collegati ad articoli

contenenti notizie riguardanti vicende giudiziarie relative a soggetti diversi dal medesimo e nei quali quest'ultimo veniva citato solamente in virtù del rapporto di parentela con i protagonisti della vicenda, non essendo dimostrato alcun suo coinvolgimento ad altro titolo. Il Garante ha accolto il ricorso ritenendo che le informazioni rese accessibili tramite il motore di ricerca fornissero, alla luce delle evidenze emerse nel corso del procedimento, un'immagine fuorviante del ricorrente senza che a ciò potesse dirsi corrispondere uno specifico interesse del pubblico a conoscere, in associazione ai suoi dati, tali informazioni, peraltro obsolete (provv. 1° marzo 2018, n. 133, doc. web n. 8475549).

In applicazione dei principi che governano la liceità del trattamento, anche i dati reperibili in rete, ed imputabili ad uno specifico titolare, devono rispondere a determinati criteri, tra i quali quello di esattezza del dato. Benché i gestori dei motori di ricerca, a differenza degli editori dei siti sui quali le notizie sono pubblicate, non possano essere ritenuti responsabili dei contenuti restituiti a seguito di ricerche condotte con il nominativo dell'interessato, il mancato aggiornamento delle informazioni in tal modo reperibili ha avuto un peso nelle valutazioni condotte dall'Autorità e ciò conformemente a quanto può desumersi dalle Linee guida sul *delisting* adottate dal Gruppo Art. 29 il 26 novembre 2014.

A questo riguardo possono citarsi due casi significativi trattati nel primo semestre del 2018. Il primo ha riguardato la richiesta di rimozione di Url collegati a notizie relative ad un procedimento penale connesso ad un'inchiesta di grande rilevanza mediatica nella quale l'interessato – residente in altro Paese collocato al di fuori dell'UE, del quale ha ottenuto la cittadinanza e nel quale ha dichiarato di svolgere in via prevalente la sua attività imprenditoriale – era stato coinvolto. Il ricorrente ha, in particolare, lamentato che tali informazioni, oltre ad essere risalenti nel tempo, non risultavano aggiornate alla luce degli esiti giudiziari successivi della vicenda, conclusasi, nei suoi riguardi, con il "patteggiamento" della pena e con la concessione dei connessi benefici di legge. Il Garante, affermata la sussistenza del proprio potere di pronunciarsi sul ricorso, ha preliminarmente contestato dalla società resistente, rappresentando come sia la direttiva europea in materia di protezione dati personali che il d.lgs. n. 196/2003 prescindano, nell'individuazione dell'ambito soggettivo di applicazione delle rispettive disposizioni, da criteri connessi alla cittadinanza o alla residenza dell'interessato ed evidenziando che, nel caso in esame, il legittimo richiamo delle relative norme dovesse ritenersi collegato all'esistenza di ragioni di interesse da individuarsi nell'ambito territoriale di visibilità dei risultati nonché nel rilievo nazionale avuto dalla vicenda giudiziaria in questione. Nel merito ha accolto l'istanza di rimozione ritenendo necessario che le informazioni diffuse in rete debbano essere esatte ed aggiornate e non ravvisando uno specifico interesse del pubblico italiano a reperire informazioni relative al ricorrente, tenuto conto del fatto che quest'ultimo svolge la sua attività in modo stabile all'estero (provv. 8 febbraio 2018, n. 72, doc. web n. 8456569).

Altro caso analogo ha portato invece il Garante a ravvisare, solo in parte, la violazione del principio di esattezza del dato con riguardo alla vicenda sottoposta alla sua attenzione – in particolare, in virtù del mancato aggiornamento del dato alla luce della successiva assoluzione pronunciata in favore dell'interessato – avuto riguardo al fatto che alcuni degli Url oggetto di richiesta di rimozione riguardavano una vicenda giudiziaria diversa, conclusasi in tempi molto recenti con la conferma in appello della condanna inflitta in primo grado al ricorrente e relativa a fatti connessi a rapporti intrattenuti dal medesimo, nella sua qualità di imprenditore edile, con enti pubblici (provv. 22 febbraio 2018, n. 110, doc. web n. 8457456).

È stata inoltre sottoposta all'attenzione dell'Autorità, sempre in questo ambito, una vicenda in cui è stata accolta, contrariamente alla posizione assunta dal titolare, la richiesta diretta ad ottenere la rimozione di Url riconducibili a contenuti che, pur avendo ad oggetto la candidatura dell'interessata all'interno di un partito politico, davano comunque conto di vicende risalenti a molti anni prima, ivi inclusi commenti e supposizioni a lei riferibili, ritenute pregiudizievoli del suo attuale percorso e la cui permanenza in rete non risultava bilanciata da un interesse attuale della collettività (provv. 15 febbraio 2018, n. 92, doc. web n. 8255869).

Trattamenti in ambito economico-finanziario e del commercio elettronico

In ambito economico si possono, tra gli altri, segnalare due casi interessanti nei quali l'Autorità si è trovata nella necessità di delineare, in modo marcato, gli ambiti di applicazione della disciplina in materia di protezione dei dati personali tenuto conto del fatto che spesso le richieste pervenute sono state dirette a ricomprendere anche aspetti attinenti a profili contrattuali del rapporto intercorrente tra le parti.

Ciò è quanto avvenuto nel caso in cui l'istanza, formalmente collegata al diritto di accesso ai dati personali dell'interessato relativi ad una polizza assicurativa, mirava, in realtà, a conoscere il prospetto di calcolo delle rivalutazioni di capitale applicato dalla compagnia. Il Garante, benché il titolare, pur eccependo l'atipicità della richiesta, abbia aderito alla stessa, ha dichiarato inammissibile il ricorso in quanto strettamente attinente ad aspetti di carattere contrattuale del rapporto e non già a conoscere dati personali del ricorrente, secondo la definizione di cui all'art. 4, comma 1, lett. *b*), del Codice (provv. 29 marzo 2018, n. 193, doc. web n. 8994724).

Vi è stato, infine, il caso di un ricorso volto ad ottenere dal titolare del trattamento, noto sito di intermediazione nell'*e-commerce*, alcune informazioni riguardanti la funzione di recensore svolta dal medesimo con riguardo a prodotti proposti in vendita tramite il portale della società resistente, ivi incluse quelle contenute nelle segnalazioni effettuate da terzi a suo carico. Il ricorrente ha chiesto, tra l'altro, il ripristino di detta funzione – revocata dalla società resistente che ha ritenuto violate alcune regole poste a tutela del corretto funzionamento del servizio – nonché la comunicazione delle motivazioni che hanno indotto la società ad effettuare tale scelta. L'Autorità ha accolto parzialmente il ricorso ordinando alla resistente di comunicare all'interessato i dati personali a lui relativi e dichiarando, invece, l'inammissibilità delle ulteriori istanze in quanto attinenti ad aspetti legati alla libertà di iniziativa economica privata della società, come tale costituzionalmente tutelata anche in ordine alle determinazioni adottate con riguardo alla prosecuzione di rapporti di tipo contrattuale (provv. 26 aprile 2018, n. 256, doc. web n. 8998681).

20 Il contenzioso giurisdizionale

20.1. *Considerazioni generali*

L'art. 10, comma 6, d.lgs. n. 150/2011, come modificato dal decreto legislativo n. 151/2018, prevede che siano notificati al Garante i ricorsi che riguardano la protezione dei dati personali ma non l'impugnazione di provvedimenti dell'Autorità.

Gli effetti di tale disposizione non si avvertono ancora sul numero delle notifiche effettuate al Garante relative a tale tipologia di giudizi: a fronte dei 12 ricorsi notificati nel 2016 e dei 14 nel 2017, nel 2018 sono stati notificati all'Autorità e da questa trattati 16 ricorsi.

Permane comunque la rilevanza dell'obbligo – purtroppo non sempre puntualmente adempiuto – per le cancellerie di trasmettere al Garante copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica (art. 154, comma 6).

Tale strumento, unitamente alle notifiche dei ricorsi, potrà consentire all'Autorità di avere conoscenza sull'evoluzione della giurisprudenza in materia di protezione dei dati personali e di svolgere il ruolo di segnalazione al Parlamento e al Governo degli interventi normativi ritenuti necessari per la tutela dei diritti degli interessati (come previsto dall'art. 154, comma 1, lett. *f*), del Codice).

20.2. *I profili procedurali*

In tema di incompetenza funzionale, la Corte di appello di Salerno, con sentenza 5 novembre 2018, n. 1702, decidendo sull'impugnazione di una sentenza del Tribunale di Salerno in materia di omesso rispetto dell'obbligo di fornire le richieste informazioni al Garante, ha dichiarato l'inammissibilità dell'appello, in quanto ai sensi dell'art. 152, comma 13, d.lgs. n. 196/2003, avverso la sentenza, si sarebbe dovuto proporre ricorso per cassazione.

Non si sono invece riscontrate pronunce che hanno dichiarato un difetto di competenza territoriale, né per materia.

20.3. *Le opposizioni ai provvedimenti del Garante*

L'anno 2018 ha registrato un sostanziale incremento nella proposizione delle opposizioni a provvedimenti dell'Autorità, 101 a fronte dei 73 ricorsi del 2017. Di queste, 59 si riferiscono a opposizioni a ordinanze ingiunzioni, in aumento rispetto alle 38 del 2017. Di seguito si dà conto delle sentenze di maggior rilievo.

Opposizioni

Complessivamente l'Autorità ha avuto notizia di 53 decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante (delle quali 39 hanno avuto ad oggetto opposizioni ad ordinanze ingiunzioni), il quale si è sempre costituito tramite l'Avvocatura dello Stato territorialmente competente.

Informativa e consenso

Tra le opposizioni alle ordinanze ingiunzioni, due decisioni hanno riguardato l'omesso consenso; in entrambi i casi, oggetto di due provvedimenti del Garante del

18 aprile 2017, n. 237 (doc. web n. 9019850) e 7 maggio 2015, n. 276 (doc. web n. 4207931), non è stato ritenuto libero e specifico il consenso raccolto a seguito delle procedure di registrazione sui rispettivi siti web delle società ricorrenti. Tale consenso, pur essendo obbligatorio, risultava indistinto rispetto alle plurime finalità del trattamento indicate nell'informativa, essendo invece necessario uno specifico consenso per ogni finalità del trattamento: in un caso, è stata applicata l'aggravante ai sensi dell'art. 164-*bis* del Codice (Trib. Trento, 12 settembre 2018, n. 826 e Trib. Trani, 19 giugno 2017, n. 1382).

Dei cinque casi che hanno riguardato l'omessa informativa e consenso, se ne segnalano due in cui due diverse società sono state sanzionate per aver effettuato un trattamento dati mediante l'invio di comunicazioni promozionali in assenza di consenso e con un'inidonea informativa. Nel primo caso, l'organo giudicante ha confermato il provv. 15 dicembre 2016, n. 536 (doc. web n. 6526145), ritenendo non completa un'informativa che non aveva evidenziato il coinvolgimento di una società operante all'estero per il servizio di invio di messaggi promozionali, benché il trasferimento dei dati non era concretamente avvenuto (Trib. Venezia, 4 maggio 2018, n. 955). Nel secondo caso, il Tribunale di Milano, con sentenza n. 9376 del 10 ottobre 2018, confermando il provvedimento 18 gennaio 2018, n. 19 (doc. web n. 8341621), ha ritenuto che le assicurazioni fornite al titolare del trattamento dalla società venditrice dei *database* di indirizzi utilizzati per le comunicazioni promozionali in merito all'informativa e all'acquisizione del consenso non integrassero l'esimente della buona fede per la ricorrente.

In entrambi i casi il giudice ha ridotto la sanzione al minimo edittale in virtù delle modalità con le quali è avvenuto il trattamento.

In altro caso, ad un esercizio commerciale è stata confermata la sanzione imposta dal Garante con il provvedimento 7 maggio 2015, n. 278 (doc. web n. 4207992) per aver omesso di rendere l'informativa mediante apposita segnalazione relativa alla presenza di sistema di videosorveglianza nel locale, a nulla rilevando la circostanza addotta dalla ricorrente che al momento dell'intervento della Guardia di finanza la telecamera fosse spenta, essendo sufficiente che attraverso il sistema sia stato effettuato un trattamento dati, anche in epoca precedente a quello dell'ispezione come accertato nel caso *de quo* (Trib. Reggio Calabria, 4 maggio 2018, n. 704).

Notificazione

Otto pronunce hanno affrontato il tema della notificazione prevista dall'art. 37 e ss. del Codice. Si dà conto delle più rilevanti.

Cinque opposizioni hanno riguardato l'omessa notificazione del trattamento effettuato con apparati di geolocalizzazione installati su autoveicoli.

In un caso, il Tribunale di Macerata ha confermato il provvedimento 9 novembre 2017, n. 468, riducendo la sanzione, in relazione al trattamento dati effettuato da una società che gestisce il servizio di trasporto pubblico locale, che ha dotato i propri automezzi di un sistema di geolocalizzazione in modo tale da consentire di risalire all'identità e alla posizione geografica del personale dipendente; al riguardo, pur ritenendo lecita la finalità del potenziamento della sicurezza pubblica, la stessa non scrimina in punto di mancata comunicazione (8 maggio 2018, n. 539).

In una seconda pronuncia, il Tribunale di Livorno ha respinto l'opposizione proposta da una società di noleggio veicoli a bordo dei quali è installato un apposito sistema automatico di rilevazione e profilazione dei clienti. Il giudice ha confermato il provvedimento 18 gennaio 2018, n. 18 (doc. web n. 8341304), ritenendo che nel trattamento effettuato dalla ricorrente ricorrono i tre elementi che caratterizzano la profilazione, ovvero l'utilizzo dei dati strettamente personali, il loro trattamento con modalità automatizzata e l'idoneità di tali dati a fornire informazioni sulle esigenze

dei clienti, non occorrendo, per l'integrazione della fattispecie, la memorizzazione *sine die* del dato acquisito e la sua associazione duratura con il singolo cliente, poiché l'attività di elaborazione attraverso un algoritmo di dati personali ulteriori rispetto a quelli necessari a fornire la prestazione base, sostanzia già di per sé un'attività di *screening* di tali dati per valutare determinati aspetti personali relativi a una persona fisica (22 novembre 2018, n. 1202).

In un terzo caso, il Tribunale di Trento ha accolto l'opposizione proposta da una società di noleggio autoveicoli e annullato l'ordinanza ingiunzione del 30 novembre 2017, n. 507 (doc. web n. 8229927), ritenendo che il Garante non abbia fornito prova che la mera presenza di un'antenna Gps consenta di per sé di geolocalizzare costantemente un veicolo, in quanto l'obbligo di cui all'art. 37 del Codice sorge quando la localizzazione effettuata con strumenti elettronici permette di individuare in maniera continuativa, anche ad intervalli, l'ubicazione sul territorio di persone o oggetti, come specificato nei "Chiarimenti sui trattamenti da notificare al Garante" del 23 aprile 2004 (24 ottobre 2018, n. 956).

Un'altra pronuncia ha riguardato un laboratorio di analisi che ha trattato dati personali senza effettuare la notifica al Garante e che ha addotto come motivo di impugnazione il fatto che il RGPD, che ha abrogato l'obbligo di comunicazione preventiva al Garante, è entrato in vigore nelle more del procedimento amministrativo che ha condotto all'irrogazione della sanzione pecuniaria, sicché il Garante si sarebbe dovuto adeguare alla normativa UE in virtù del principio di retroattività della *lex mitior* ricavabile dall'art. 7 CEDU. Il giudice, confermando il provvedimento del Garante dell'11 maggio 2017, n. 230 (doc. web n. 6703871) ma riducendo ai minimi edittali la sanzione, ha ritenuto, anche alla luce di una costante giurisprudenza della Corte costituzionale in merito alla legittimità dell'art. 1, l. n. 689/1981, di escludere l'applicazione del suddetto principio (Trib. Verona, 10 aprile 2018, n. 867).

Il giudice ha confermato il provvedimento del Garante del 1° marzo 2018, n. 130 (doc. web n. 8999305), che ha sanzionato un'agenzia investigativa per non aver notificato l'utilizzo di Gps relativo agli spostamenti compiuti dal soggetto non ravvisando un errore scusabile, alla luce della giurisprudenza sulla presunzione di colpa a carico del trasgressore. Tantomeno fondato è stato ritenuto il rilievo interpretativo volto ad escludere il Gps dall'ambito applicativo dell'art. 37 del Codice e la considerazione che la continuità del rilevamento venga meno per il fatto che ci possano essere interruzioni o intervalli nell'individuazione dell'ubicazione del soggetto. È stata tuttavia ridotta la sanzione su richiesta di parte ricorrente in considerazione del fatto che non si trattava di dati sensibili; che il RGPD, seppur non ancora in vigore al momento della commissione dell'illecito, non prevede più la previa notificazione al Garante, diminuendo di fatto il disvalore della relativa condotta omissiva; che il titolare del trattamento ha provveduto alla comunicazione dei dati trattati nella fase immediatamente successiva alla relativa segnalazione; che l'agenzia investigativa abbia regolare autorizzazione ministeriale e non risulta accertata alcun altra violazione in materia di protezione dati (Trib. Pavia, 18 luglio 2018, n. 1235).

Infine la Cassazione ha accolto il ricorso del Garante avverso la sentenza del Tribunale di Catania che aveva annullato l'ordinanza ingiunzione del 15 novembre 2012, n. 345 (doc. web n. 2284794) per omessa notificazione ex art. 37 del Codice, oltreché omesso consenso, informativa e misure di sicurezza, emessa nei confronti di una società in relazione ad un sistema di raccolta di dati biometrici della mano per la rilevazione delle presenza dei dipendenti, ritenendo irrilevante, ai fini della configurabilità del trattamento di dati personali, la mancata registra-

20

Trattamenti da parte di soggetti pubblici

zione degli stessi in apposita banca dati, essendo sufficiente anche un'attività di raccolta ed elaborazione temporanea ed essendo altresì irrilevante il fatto che il modello archiviato consista in un algoritmo unidirezionale e irreversibile (4 maggio 2018, n. 25686).

Nove opposizioni hanno riguardato il trattamento dati da parte di soggetti pubblici e in otto casi, di seguito sinteticamente analizzati, si è trattato di pubblicazione di dati sensibili su siti istituzionali.

Nel primo caso, il Tribunale de L'Aquila, ha confermato il provvedimento 6 aprile 2017, n. 179 (doc. web n. 6521730), respingendo l'opposizione proposta da un Ente territoriale che aveva diffuso dati idonei a rivelare lo stato di salute tramite pubblicazione sul proprio sito istituzionale di candidati disabili ammessi e non ammessi in relazione ad una selezione pubblica; il giudice ha ritenuto che il trattamento dati poteva essere effettuato dall'opponente in forma anonima o in modo da contemperare le esigenze di pubblicità della procedura concorsuale con quelle di riservatezza dei candidati (30 aprile 2018, n. 355).

Analogamente in altro caso, è stato confermato il provvedimento 10 novembre 2016, n. 465 (doc. web n. 6531740) in relazione alla pubblicazione dei dati personali dei bambini ammessi e non al servizio di trasporto scolastico, ritenendo il giudice che l'obbligo di trasparenza poteva essere assolto garantendo un accesso selettivo agli utenti realmente interessati e che in ogni caso i dati pubblicati risultano sovrabbondanti rispetto alle finalità perseguite con la pubblicazione (Trib. Torre Annunziata, 28 giugno 2018, n. 1571).

Nel terzo caso, il Tribunale di Lecce ha confermato il provvedimento 21 dicembre 2017, n. 563 (doc. web n. 7968336), con il quale il Garante aveva sanzionato un ente locale in relazione alla pubblicazione nell'albo pretorio dell'elenco degli ammessi all'esonero del pagamento della mensa scolastica, ritenendo che i dati indicati consentissero di ricavare informazioni circa le condizioni economiche gravemente precarie dei soggetti esentati. La sanzione è stata ridotta in considerazione del fatto che il trattamento è avvenuto per finalità sociali a favore dei soggetti cui le violazioni si riferivano (13 novembre 2018, n. 9554).

In altro caso, il Tribunale di Bari ha confermato il provvedimento 12 marzo 2015, n. 152 (doc. web n. 3999853), giudicando illecita la pubblicazione sul sito istituzionale di un Comune di alcune ordinanze sindacali relative al trattamento sanitario obbligatorio di una persona, ritenendo che la finalità di tutelare la pubblica incolumità e sicurezza dei cittadini avanzata dall'ente territoriale interessato potesse essere perseguita con la stessa efficacia anche senza indicare la patologia del soggetto. La sanzione è stata ridotta, avendo il giudice riconosciuto la sproporzione tra fatto contestato e sanzione comminata (9 luglio 2018).

Il Tribunale di Tempio Pausania, ha confermato il provvedimento 1° ottobre 2015, n. 513 (doc. web n. 4667456), in relazione alla pubblicazione sul sito istituzionale di un comune di una delibera contenente dati sulla salute di una dipendente, ritenendo che la diffusione dell'informazione sull'assenza per malattia costituisca dato sensibile pur in assenza dell'indicazione di una patologia, conformemente a quanto affermato dalla Cassazione con sentenza n. 1898/2013 (9 febbraio 2018, n. 42).

In due casi il giudice ha confermato i provvedimenti del Garante, rispettivamente del 5 ottobre 2017, n. 397 (doc. web n. 7309596) e 398 (doc. web n. 7309671) che hanno sanzionato l'ente territoriale ricorrente per aver pubblicato due distinte deliberazioni contenti dati personali oltre il termine quindicinale previsto per legge (Trib. Aosta, 3 maggio 2018, nn. 126 e 127). Mentre in un altro caso l'organo giudicante non ha ritenuto sussistente la prova sull'autore sostanziale della violazione

ravvisata nel provvedimento 28 luglio 2016, n. 340 (doc. web n. 5562422) che è stato pertanto annullato, risultando che il contenuto oggetto di pubblicazione era stato regolarmente rimosso dal sito istituzionale dell'ente locale entro il termine previsto per legge e che il comune ricorrente ha provveduto ad effettuare tutti gli adempimenti previsti dalla normativa vigente (Trib. Viterbo, 14 febbraio 2018, n. 266).

Ulteriori casi

In un caso il Tribunale di Catania ha accolto l'impugnazione del provvedimento 7 aprile 2011, n. 135 (doc. web n. 1857022) che aveva sanzionato sotto il profilo amministrativo per omesse misure di sicurezza un'azienda ospedaliera, benché una sanzione fosse già stata irrogata per la stessa fattispecie al rappresentante legale della suddetta azienda che aveva provveduto al pagamento. Il giudice ha ritento trattarsi di un concorso eterogeneo di norme, poiché per la medesima condotta sono previste sia la sanzione amministrativa che quella penale. Pertanto, in virtù dell'art. 162-*bis* del Codice, che esclude la sanzione amministrativa qualora il fatto costituisca reato, nonché dell'art. 9, l. n. 689/1981, che dispone la prevalenza della disposizione speciale, nel caso considerato, quella penale in quanto prevede la possibilità di estinguere il reato attraverso l'adempimento di quanto era stato omesso e il pagamento della sanzione, ha ritenuto pertanto che la sanzione irrogata al rappresentante legale era l'unica ammissibile (13 dicembre 2016, n. 6016).

In altro caso, una società ha contestato la nullità del provvedimento 12 febbraio 2015, n. 82, in quanto notificato a mezzo di posta elettronica certificata, risultando la relata priva di firma digitale e di identificazione non privilegiata dell'agente notificatore. Il giudice, riportandosi ad una giurisprudenza consolidata, ha confermato l'ordinanza ingiunzione, ritenendo la nullità della notifica del verbale di accertamento delle violazioni amministrative sanata dal raggiungimento dello scopo, nel caso di specie dalla conoscenza dell'atto attraverso la consegna telematica, secondo quanto previsto dal codice di rito (Cass. civ. 11 aprile 2018, n. 22906).

La Cassazione (7 marzo 2018, n. 15332), annullando la sentenza del Tribunale di Santa Maria Capua Vetere che aveva ritenuto necessario un collegamento tra la condotta omissiva, concretizzatasi nella mancata risposta alla richiesta di informazioni, e la sussistenza della violazione segnalata, ha deciso che tale collegamento non fosse previsto dalla legge che punisce espressamente la sola condotta omissiva a fronte di specifica richiesta del Garante e che la norma sanzionatoria (art. 164 del Codice) non appare sospetta di illegittimità costituzionale, come adombrato dal Tribunale, in quanto l'obbligo di collaborazione con soggetti pubblici deputati all'accertamento di illeciti amministrativi è previsto in vari settori dell'ordinamento e l'ammontare della sanzione non pone dubbi di costituzionalità ma testimonia l'interesse del legislatore a stimolare la collaborazione con un organo pubblico preposto alla tutela di diritti personali di eminente rilievo costituzionale. Viene confermato, pertanto, il provvedimento del Garante del 19 settembre 2013, n. 508 (doc. web n. 3033451).

Diritto all'identità personale

In tema di trattamento da parte dei motori di ricerca il Tribunale di Milano ha respinto il ricorso di Yahoo Emea Limited avverso la decisione del 26 gennaio 2017, n. 30 (doc. web n. 6026501) con la quale il Garante, accogliendo il ricorso dell'interessato, aveva ordinato al motore di ricerca la deindicizzazione di alcuni dati personali.

La sentenza, evidenzia, in armonia con la decisione della CGUE 13 maggio 2014 (*Costeja*) secondo cui il motore di ricerca è titolare del trattamento e non mero intermediario, ed in linea con CGUE 1° ottobre 2015 (*Weltimmo*), che qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile, può rilevare ai fini del collegamento giurisdizionale. Nella specie, la diffusione dei dati sul web era avvenuta prima della cessazione dell'attività da parte di Yahoo! Italia, che svolgeva attività di supporto idonea a farla considerare quale stabilimento

di Yahoo! Emea, insediata in Irlanda ed alla quale fa capo l'attività del motore di ricerca. La sentenza poi chiarisce che "[…] precludere l'accesso alla tutela dinanzi all'Autorità garante per la privacy italiana comporterebbe una lesione del diritto ad una tutela effettiva, e che tale non sarebbe quella assicurata dall'Autorità irlandese", e che la possibilità di ricorrere al Garante nazionale, che dovrebbe poi riconoscere il proprio dovere di collaborazione con altra autorità nazionale ritenuta competente, si risolve in una forma di tutela soltanto apparente (22 gennaio 2018, n. 491).

Sempre in tema di motori di ricerca, il Tribunale di Milano, su domanda di Google LLC e Google Italy s.r.l., ha annullato la decisione del Garante del 21 dicembre 2017, n. 557 (doc. web n. 7465315) con la quale, ritenuto sussistente il diritto all'oblio, era stato accolto il ricorso dell'interessato volto alla deindicizzazione globale di alcuni Url. La sentenza si sofferma anzitutto sulla natura oggettiva della situazione giuridicamente tutelata dedotta in giudizio, osservando che la natura diffamatoria dei contenuti di alcuni dei *link* oggetto del ricorso non può essere esaminata in via principale nel procedimento, avente ad oggetto esclusivamente l'asserita lesione del diritto all'identità personale e la tutela chiesta nei confronti del motore di ricerca Google, poiché spetta al giudice ordinario – e non al gestore del motore di ricerca – operare il bilanciamento tra diritto all'onore o alla reputazione e diritto alla libertà di manifestazione del pensiero (5 settembre 2018, n. 7846). Evidenzia poi che l'esame delle domande formulate dall'interessato – aventi ad oggetto la tutela di un diritto e non un mero sindacato sulla legittimità di un atto amministrativo – debba essere riferito all'attualità, tenendo conto dei documenti e delle risultanze emerse anche in epoca successiva all'adozione del provvedimento da parte del Garante. Sottolinea quindi che l'interessato, professore universitario ed imprenditore (circostanze già note all'epoca in cui è stato adottato il provvedimento impugnato), era stato altresì candidato alle ultime elezioni politiche nelle circoscrizioni del Centro e Nord America, rivestendo così un ruolo pubblico. Al riguardo, da inchieste giornalistiche prodotte dalla difesa delle società ricorrenti, era emerso che i titoli di studio indicati dall'interessato risultavano non veritieri, che l'istituto presso il quale aveva dichiarato di aver avuto una docenza sembrava inesistente e che lo stesso interessato veniva descritto come molestatore seriale ed autore di comportamenti molesti ovvero diffamatori, sicché non potevano ritenersi inesatti in termini reali i dati personali riferiti all'interessato, da ritenersi invece pertinenti e completi. Il Tribunale per tali ragioni ha accolto il ricorso delle società. Essendo stati utilizzati documenti di formazione successiva al deposito del provvedimento del Garante, nei rapporti tra le società ricorrenti e l'Autorità è stata disposta la integrale compensazione delle spese di lite.

Altra pronuncia ha riguardato la pubblicazione su un quotidiano *online* di un articolo nel quale veniva riportato un documento riguardante un noto personaggio nell'esercizio della propria attività professionale con informazioni ritenute false e diffamatorie e delle quali la ricorrente ha richiesto il blocco e l'eliminazione dal sito. Il Tribunale di Roma, confermando pienamente il provvedimento del Garante del 7 febbraio 2012, ha richiamato la giurisprudenza in materia del cd. diritto di intervista, secondo cui il giornalista può lecitamente riportare dichiarazioni altrui qualora assuma una posizione imparziale di terzo osservatore e qualora le dichiarazioni offensive in ragione dell'interesse pubblico all'informazione, prevalgano sull'interesse del singolo e legittimino l'esercizio del diritto di cronaca. Nel caso di specie, le dichiarazioni, pur non frutto di un'intervista, sono contenute in un *dossier* elaborato da un soggetto individuato e rientrano nella scriminante considerata, in quanto riportano testimonianze di colleghi che hanno scelto l'anonimato. Il provvedimento del Garante è stato ritenuto legittimo anche nella parte in cui ha considerato adem-

piuto l'obbligo di dare adeguata diffusione alla lettera di scuse dell'autore del dossier che ha dato conto della falsità delle notizie in esso riportate, in attuazione dei principi di correttezza nonché esattezza, aggiornamento e completezza (17 ottobre 2013, n. 20867).

In tema di consenso è stato accolto dalla Suprema Corte il ricorso presentato dal Garante contro la sentenza del Tribunale di Arezzo del 29 aprile 2016 che aveva accolto l'opposizione proposta da una società contro il provvedimento 25 settembre 2014, n. 427 (doc. web n. 3457687) con il quale, tra l'altro, era stato dichiarato illecito il trattamento dei dati personali posto in essere per finalità promozionali senza aver ottenuto un consenso libero e specifico degli interessati ex artt. 23 e 130 del Codice.

In particolare, secondo la Corte deve escludersi che il consenso possa dirsi specificamente, e dunque anche liberamente, prestato in un'ipotesi in cui, ove gli effetti del consenso non siano indicati con completezza accanto ad una specifica "spunta" apposta sulla relativa casella di una pagina web, ma siano invece descritti in altra pagina web linkata alla prima, non vi sia contezza che l'interessato abbia consultato detta altra pagina, apponendo nuovamente una diversa "spunta" finalizzata a manifestare il suo consenso. In termini più generali, ha chiarito la Corte, "in tema di consenso al trattamento dei dati personali, la previsione dell'articolo 23 del Codice della *privacy*, nello stabilire che il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, consente al gestore di un sito internet, il quale somministri un servizio fungibile, cui l'utente possa rinunciare senza gravoso sacrificio (nella specie servizio di *newsletter* su tematiche legate alla finanza, al fisco, al diritto e al lavoro), di condizionare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie, sempre che il consenso sia singolarmente ed inequivocabilmente prestato in riferimento a tale effetto, il che comporta altresì la necessità, almeno, dell'indicazione dei settori merceologici o dei servizi cui i messaggi pubblicitari saranno riferiti" (11 maggio 2018, n. 17278).

Sempre in tema di omesso consenso, il Tribunale di Milano ha confermato il provvedimento del Garante del 26 ottobre 2017, n. 439 (doc. web n. 7339171), in relazione all'attivazione per errore di un servizio da parte di una compagnia telefonica ad un cliente senza richiederne il consenso. Il giudice ha ritenuto che dall'errore che ha determinato il trattamento illecito non può discendere l'inapplicabilità della disciplina in materia di trattamento dati, in particolare riguardo agli obblighi di informativa e consenso, ma l'elemento soggettivo dell'agente rileverà solo nella valutazione della sua responsabilità e applicabilità dell'eventuale provvedimento sanzionatorio, non oggetto del giudizio (7 giugno 2018, n. 6460).

In altro caso, il Garante, con provvedimento 24 novembre 2016, n. 488 (doc. web n. 5796783), ha disposto il divieto di trattamento dei dati personali nei confronti di una Associazione che attribuisce *rating* reputazionali a persone fisiche e giuridiche attraverso un sistema di elaborazione di processi matematici che parte dal volontario caricamento sulla piattaforma *web* da parte degli utenti di documenti significativi, in assenza di una idonea cornice normativa che renda lecito il trattamento, e di un consenso espresso liberamente.

Il giudice, dopo essersi espresso sulla natura esclusiva della giurisdizione ordinaria che prescinde dalla situazione soggettiva per cui si agisce, ha accolto il ricorso promosso dall'Associazione, ritenendo che la mancanza di una disciplina normativa istitutiva del *rating reputazionale* non comporta il difetto di liceità del Sistema di elaborazione dati utilizzato, in quanto consono ai principi dell'autonomia privata; anche il consenso può ritenersi prestato lecitamente, poiché le attività di carica-

mento delle informazioni e di validazione delle certificazioni dei documenti sono soggette al consenso dell'interessato, riconoscendo invece una criticità del sistema in relazione agli effetti di circolazione e conoscibilità dei dati personali relativi a terzi mancando il requisito del consenso degli interessati e permanendo, dunque sotto quest'ultimo profilo, il divieto disposto dal citato provvedimento del Garante in ordine alle attività riferibili al trattamento personale di terzi. Avverso la sentenza pende giudizio davanti alla Corte di cassazione promosso dal Garante (Trib. Roma, 4 aprile 2018, n. 5715).

Una pronuncia ha confermato il provvedimento del Garante dell'8 maggio 2014, n. 231 (doc. web n. 3275922), che ha dichiarato illecita la comunicazione effettuata da una compagnia assicurativa nei confronti di un agenzia investigativa al fine di compiere accertamenti in relazione allo stato di salute di un minore, in quanto nel bilanciamento di interessi il diritto che la società potrebbe far valere in giudizio è di natura esclusivamente patrimoniale, e dunque in base al principio del pari rango tale interesse non può ritenersi prevalente sulla necessità di tutela i dati relativi alla salute del minore (Trib. Bologna, 8 novembre 2017, n. 61).

In altro caso, il Tribunale di Torino ha confermato il provvedimento 7 agosto 2017, n. 298 (doc. web n. 9023957), ritenendo che la Banca avesse acquisito legittimamente i dati dei ricorrenti in qualità di soci e garanti di una società da anni in contenzioso con l'istituto bancario, essendo tali dati strettamente necessari per l'effettuazione delle operazioni richieste; il perdurante possesso da parte della Banca dei suddetti dati, peraltro meramente identificativi della persona del ricorrente, deve ritenersi legittimo in virtù dell'interesse a conservare la storia dei rapporti contrattuali in essere tra le parti. È stato ritenuto infondato altresì il rilievo di un accesso abusivo alla Centrale rischi presso la Banca d'Italia, in quanto il creditore è perfettamente legittimato ad accedere ai dati relativi alla situazione debitoria, accesso che comunque nel caso di specie ha riguardato la società di cui i ricorrenti erano soci e garanti e non le persone fisiche (14 febbraio 2018, n. 769).

Il Tribunale di Milano, confermando il provvedimento 2 novembre 2017, ha ritenuto che il trattamento di dati giudiziari effettuato da una società nei confronti di appaltatori e subappaltatori del Gruppo, che si è concretizzato in uno *screening* reputazionale, fosse privo di una base di legittimazione, non essendo tali le disposizioni del Codice antimafia richiamate dalla medesima società, che invece si limitano a prescrivere in capo a soggetti determinati accertamenti specifici che, pur non essendo necessariamente tipizzati, non contemplano mai l'espressa autorizzazione al trattamento dati giudiziari; neppure l'interesse perseguito, rappresentato dalla necessità di prevenire comportamenti fraudolenti e corruttivi nonché altre condotte illecite a tutela dell'integrità e l'immagine delle società del Gruppo, è stato ritenuto potersi porre a fondamento del trattamento dei dati giudiziari in quanto carente del duplice requisito della "specificità" e della "pubblicità" secondo quanto previsto dall'art. 27 del Codice (Trib. di Milano, 20 novembre 2018, n. 9890).

20.4. *L'intervento del Garante nei giudizi relativi all'applicazione del Codice*

Conformemente agli indirizzi giurisprudenziali e al parere espresso dall'Avvocatura generale dello Stato, il Garante, nei giudizi diversi da quelli direttamente attinenti a pronunce dell'Autorità, ha limitato la propria attiva presenza ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari questioni di diritto.

In questo quadro, l'Autorità ha comunque seguito con attenzione tutti i conten-

ziosi nei quali non ha ritenuto opportuno intervenire, chiedendo all'Avvocatura dello Stato di essere comunque informata sullo svolgimento delle vicende processuali e di ricevere comunicazione in merito agli esiti.

Al riguardo si consideri che la notifica al Garante dei ricorsi in materia di protezione dei dati personali che non riguardano provvedimenti dell'Autorità amplia la casistica di possibile intervento, anche in relazione a questioni di legittimità costituzionale o di compatibilità europea di leggi, anche con riferimento alla Carta dei diritti fondamentale dell'Unione europea (CDFUE), nonché alle norme di adeguamento al RGPD, in relazione a disposizioni la cui difesa per conto della Presidenza del Consiglio dei ministri è affidata all'avvocatura erariale. La legittimazione attiva dell'Autorità nei giudizi in cui non è parte ed il potere di intervento al fine di sostenere principi rilevanti nell'applicazione della disciplina in materia di protezione dei dati personali, sembrerebbero potersi desumere anche dall'art. 154-*ter* del Codice, nella parte in cui ora riconosce al Garante la legittimazione ad agire nei confronti del titolare o del responsabile del trattamento *tout court*, senza alcuna qualificazione, "in caso di violazione delle disposizioni in materia di protezione dei dati personali.

Il menzionato art. 154-*ter* del Codice (nuova formulazione), attribuendo la rappresentanza in giudizio del Garante all'Avvocatura generale dello Stato ai sensi dell'art. 1, r.d. n. 1611/1933, prevede che, nei casi di conflitto di interesse, il Garante, sentito l'Avvocato generale dello Stato, può stare in giudizio tramite propri funzionari iscritti nell'elenco speciale degli avvocati dipendenti di enti pubblici ovvero avvocati del libero foro.

Pertanto, l'Autorità ha svolto approfondimenti sia sulla possibilità di istituire un'avvocatura interna, sia sull'istituzione di un elenco di avvocati del libero foro nel quale scegliere a chi affidare di volta in volta il patrocinio delle controversie, in ragione dell'eventuale conflitto di interessi che dovesse presentarsi quando la controparte è un'autorità pubblica. Ciò, tenendo conto dei recenti e rigorosi orientamenti del Consiglio di Stato (parere 9 aprile 2018, n. 2017) e della Corte dei conti (deliberazione 22 maggio 2018, n. 105), che impongono alle amministrazioni pubbliche di procedimentalizzare la scelta del professionista al quale affidare di volta in volta l'incarico di rappresentanza in giudizio, affinché sia garantito il rispetto dei principi di economicità, efficacia, imparzialità, parità di trattamento, trasparenza, proporzionalità e pubblicità, di cui all'art. 4 del Codice dei contratti pubblici (d.lgs. 18 aprile 2016, n. 50).

Occorre ancora considerare che in base al nuovo testo del Codice l'autorità giudiziaria deve comunicare al Garante la pendenza di una controversia, trasmettendo copia degli atti introduttivi (art. 10, comma 9, d.lgs. 1° settembre 2011, n. 150, come modificato dall'art. 17, d.lgs. n. 101/2018). Tale comunicazione consente all'Autorità, "nei casi in cui non sia parte in giudizio", di "presentare osservazioni, da rendere per iscritto o in udienza, sulla controversia in corso con riferimento ai profili relativi alla protezione dei dati personali".

21 L'attività ispettiva e le sanzioni

21.1. *Il nuovo quadro normativo di riferimento sui poteri di indagine del Garante*

L'attività ispettiva è lo strumento istruttorio necessario sia per accertare *in loco* situazioni di fatto oggetto di valutazione da parte dell'Autorità in relazione a specifici casi, sia per acquisire conoscenze relative a fenomeni nuovi in vista di successivi interventi da parte del Garante nell'ambito delle attribuzioni allo stesso rimesse dal RGPD e dal Codice.

Più precisamente, lo svolgimento della funzione ispettiva riguarda un complesso di poteri autoritativi nell'ambito dei quali il Garante realizza le attività di controllo e di ricerca di notizie e prove volte a verificare la corretta applicazione delle disposizioni in materie di protezione dei dati personali.

Tali poteri, già previsti nella direttiva 95/46/CE (cfr. art. 28, par. 3), sono ora rinvenibili anche nel RGPD, il quale individua tra i compiti delle autorità di protezione dei dati lo svolgimento di "indagini sull'applicazione del regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica" (artt. 57, par. 1, lett. *h*); 58, par. 1), prevedendo espressamente che l'autorità di controllo abbia specifici poteri di indagine, tra i quali quelli di ingiungere il rilascio di ogni informazione necessaria per l'esecuzione dei suoi compiti; ottenere l'accesso a tutti i dati personali e a tutte le informazioni essenziali per l'esecuzione dei suoi compiti; ottenere l'accesso a tutti i locali, compresi tutti gli strumenti e i mezzi di trattamento dei dati.

Il legislatore nazionale, novellando (con il d.lgs. n. 101/2018) le specifiche disposizioni del Codice, ha adeguato l'ordinamento italiano alle previsioni del RGPD anche nello specifico settore dei controlli, dotando il Garante di poteri di controllo e di accertamento diversi per grado di "invasività" e per efficacia.

Da una parte, infatti, è stato previsto che il Garante possa richiedere informazioni e documenti al titolare, al responsabile (e ora anche ai relativi rappresentanti), agli interessati e anche a terzi, in un'ottica di collaborazione fra organi incaricati di acquisire le informazioni e soggetti ispezionati. Dall'altra, è stato stabilito che l'Autorità possa disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali, avvalendosi, se del caso, anche di strumenti di polizia giudiziaria.

Sotto altro profilo, il RGPD amplia notevolmente gli spazi di collaborazione tra le autorità di controllo, prevedendo che le stesse debbano fornirsi assistenza reciproca, anche per realizzare accessi nell'ambito delle "operazioni congiunte delle autorità di controllo". È previsto, infatti, che tali operazioni avvengano mediante lo svolgimento, in collaborazione, di indagini e controlli nei confronti di un titolare o di un responsabile del trattamento stabilito in un altro Stato membro. In tale eventualità, l'autorità di controllo competente invita l'autorità di controllo dello Stato membro interessato a partecipare all'operazione congiunta e risponde, con reciprocità, alle richieste di partecipazione delle altre autorità di controllo. In tale contesto di reciprocità, costituisce una specifica ulteriore novità la circostanza che un'autorità di controllo possa, in conformità al proprio diritto interno e con l'au-

torizzazione dell'autorità di controllo ospitata, conferire poteri, anche d'indagine, al personale o ai membri dell'autorità di controllo ospitata che partecipino alle operazioni congiunte, o consentire ai membri o al personale dell'autorità di controllo ospitata, nella misura in cui il diritto interno lo permette, di esercitare i loro poteri d'indagine in conformità al diritto dello Stato membro dell'autorità di controllo ospitata.

Inoltre, costituisce una novità la possibilità che, sulla base di apposite garanzie, il Garante possa effettuare accertamenti in luoghi privati per il controllo su reti di comunicazione accessibili al pubblico e acquisire dati e informazioni *online.*

Nella disamina dei poteri di indagine riconducibili al Garante, appartengono ai "particolari accertamenti" quelli riguardanti i trattamenti effettuati per motivi di sicurezza e difesa dello Stato. Tali indagini sono effettuate per il tramite di un componente designato dal Garante e i documenti acquisiti in tali circostanze sono custoditi assicurandone la segretezza e sono conoscibili dal presidente e dai componenti del Garante nonché, se necessario, da un numero delimitato di addetti all'Ufficio individuati dal Garante. Per gli accertamenti relativi invece agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.

Appare utile rimarcare che il mancato riscontro alla richiesta di informazioni ovvero il negato accesso ai dati e ai locali configurano una violazione amministrativa sanzionata fino a 20.000.000 euro o, per le imprese, fino al 4% del fatturato.

È poi considerato particolarmente grave, configurando addirittura illecito penale punito con la reclusione da sei mesi a tre anni, il comportamento di colui che, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiari o attesti falsamente notizie o circostanze o produca atti o documenti falsi. Non meno grave è considerata, infine, l'intenzionale interruzione o la turbativa della regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti, punita con la reclusione sino ad un anno.

A fronte della descritta "invasività" dei poteri di indagine, lo stesso RGPD dispone che ogni Paese disponga di "garanzie appropriate per l'esercizio del potere dell'Autorità nello svolgimento delle attività ispettive e di controllo". Nel nostro ordinamento talune specifiche disposizioni contenute nel Codice prevedono che, qualora gli accertamenti siano svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, siano effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento.

21.2. *La programmazione dell'attività ispettiva nel 2018*

Le ispezioni, pari a 150 nel 2018, sono state effettuate sulla base di programmi elaborati secondo linee di indirizzo stabilite dal Collegio con delibere di programmazione recanti gli ambiti del controllo e gli obiettivi numerici da conseguire. Le linee generali della programmazione dell'attività ispettiva sono state quindi rese pubbliche attraverso il sito web del Garante (*newsletter* 28 febbraio 2018 n. 438, doc. web n. 7835687; *newsletter* 31 luglio 2018, n. 443, doc. web n. 9025406) e, sulla base dei criteri così fissati, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo e istruisce i conseguenti procedimenti.

Il programma relativo al 2018 ha previsto che l'attività ispettiva fosse indirizzata, in particolare, nei seguenti settori:

– trattamenti di dati personali effettuati da società/enti che gestiscono banche dati di rilevanti dimensioni;

– trattamenti di dati sanitari effettuati dalle aziende sanitarie locali, in relazione al trasferimento degli stessi in favore di terzi per il loro utilizzo a fini di ricerca;

– trattamenti di dati personali effettuati presso istituti di credito relativamente alla legittimità della consultazione e del successivo utilizzo di dati da parte di soggetti aventi diritto, anche in riferimento al tracciamento degli accessi e a correlate misure di protezione;

– trattamenti di dati effettuati da società per attività di *rating* sul rischio e sulla solvibilità delle imprese;

– trattamenti di dati personali effettuati da società per attività di telemarketing in relazione alle numerose segnalazioni pervenute all'Autorità.

Come specificato al par. 21.4, nel periodo di riferimento sono state effettuate verifiche anche in altri settori,:

– sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;

– sulla liceità e correttezza dei trattamenti di dati personali, con particolare riferimento al rispetto dell'obbligo di informativa, alla pertinenza e non eccedenza nel trattamento, alla libertà e validità del consenso, nei casi in cui questo è necessario, nonché alla durata della conservazione dei dati nei confronti di soggetti, pubblici o privati, appartenenti a categorie omogenee.

In tutta l'attività è stata prestata specifica attenzione ai profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate.

21.3. *La collaborazione con la Guardia di finanza*

Anche nell'anno di riferimento l'Autorità si è avvalsa della preziosa collaborazione della Guardia di finanza per lo svolgimento delle attività di controllo. Il consolidato rapporto con il Corpo consente al Garante di disporre di risorse qualificate in grado di supportare l'attività ispettiva sull'intero territorio nazionale attraverso:

– la partecipazione di personale ad accessi a banche dati, ispezioni, verifiche e altre rilevazioni nei luoghi ove si svolge il trattamento;

– l'assistenza nei rapporti con l'autorità giudiziaria;

– lo sviluppo di attività ispettive delegate o subdelegate per l'accertamento delle violazioni;

– la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate (attività svolta fino al 25 maggio 2018, secondo il regime previsto dalla legge 24 novembre 1981, n. 689; successivamente a tale data, per effetto del RGPD, tale potere è in capo esclusivamente al Garante);

– l'esecuzione di indagini conoscitive sullo stato di attuazione della legge in determinati settori;

– la segnalazione all'Autorità di situazioni rilevanti, ai fini dell'applicazione della legge, acquisite anche nell'esecuzione di altri compiti di istituto.

In linea generale, appare utile evidenziare che il protocollo di intesa tra il Garante e la Guardia di finanza, sottoscritto inizialmente il 26 settembre 2002 e successivamente rinnovato più volte, si colloca nel solco dei consolidati rapporti di collaborazione tra i due Enti. Il nuovo protocollo d'intesa in corso di aggiornamento, disporrà l'adeguamento del testo alle modifiche di carattere normativo ed al nuovo assetto

organizzativo dei Reparti speciali che, a decorrere da luglio 2018, ha visto la soppressione del Nucleo speciale *privacy* e l'istituzione del "Nucleo speciale tutela *privacy* e frodi tecnologiche", testimoniando gli ottimi risultati sin qui ottenuti dalla suddetta collaborazione ed è finalizzato ad assicurare il sostegno ad un comparto delicato come quello della tutela dei dati personali. Tale rinnovata collaborazione, prevede anche l'aumento del personale distaccato presso il Garante da quattro a sei unità, consentirà all'Autorità, anche grazie all'apporto della nuova unità speciale che ingloba le competenze in ambito tecnologico, di avvalersi di un efficace sostegno allo svolgimento delle proprie funzioni ispettive, conoscitive ed informative sui fenomeni che riguardano, nei contesti pubblici e privati, il trattamento dei dati personali.

Il nuovo protocollo d'intesa prevede inoltre, dal punto di vista strategico, che il Garante possa avvalersi di personale specializzato del Corpo anche per la conduzione di ispezioni congiunte con altre autorità estere.

Da un punto di vista più strettamente operativo, invece, l'adozione del protocollo ha finora consentito: una sempre maggiore semplificazione dei flussi documentali tra l'Ufficio e il Nucleo speciale tutela *privacy* e frodi tecnologiche (attraverso l'uso sistematico di strumenti di trasmissione telematici); l'introduzione di modalità di verifica *online* di possibili violazioni alla normativa in materia di protezione dei dati personali (attraverso l'esame diretto di siti web, senza necessità di ispezioni *in loco*). Sulla base del suddetto protocollo, le informazioni e i documenti acquisiti nell'ambito degli accertamenti effettuati dal Corpo sono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge. Qualora nell'ambito dell'ispezione emergano violazioni penali, la Guardia di finanza procede direttamente alla segnalazione della notizia di reato all'autorità giudiziaria.

Anche nell'anno 2018, nei casi in cui sono emerse violazioni penali o amministrative, la Guardia di finanza ha provveduto a informare l'autorità giudiziaria competente (n. 14 violazioni penali accertate) e ad avviare i procedimenti sanzionatori amministrativi (n. 488 violazioni amministrative contestate) mediante la redazione dell'atto di contestazione, in conformità alla citata legge n. 689/1981.

Infine si rileva anche nel corso del 2018 la prosecuzione dell'attività di formazione del personale del Corpo al fine di approfondire la conoscenza delle disposizioni del Codice e dei provvedimenti dell'Autorità, come previsto dal citato protocollo d'intesa, nonché, in particolare, gli approfondimenti effettuati in merito alle novità legislative introdotte dal RGPD e dal decreto legislativo n. 101/2018.

Si può quindi osservare che, grazie alla sinergia ormai collaudata con il Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza, il Garante dispone di un dispositivo di controllo flessibile ed articolato, in grado di integrare l'attività ispettiva svolta direttamente dal competente dipartimento dell'Autorità, consentendo così l'effettuazione, efficace e tempestiva, di tutte le verifiche *in loco* che si rendono necessarie per garantire il rispetto della protezione dei dati personali su tutto il territorio nazionale.

21.4. *I principali settori oggetto di controllo*

Oltre a quanto già riportato al par. 21.2, le ispezioni effettuate dall'Autorità nel 2018 hanno riguardato le seguenti categorie di titolari del trattamento:

– enti pubblici vari (in particolare comuni e regioni), in relazione al trattamento di dati personali svolto mediante le cd. *app* per *smartphone* o *tablet,* al fine di verificare, nell'ambito dei diversi servizi offerti, le categorie di dati raccolti e le tipologie

di trattamenti effettuati, tra cui, in particolare, l'eventuale profilazione o geolocalizzazione degli interessati, le misure di sicurezza previste e l'eventuale comunicazione di dati personali a terzi;

– società ed altri operatori economici, con riferimento ai trattamenti di dati personali raccolti attraverso l'utilizzo di siti web, per la verifica delle modalità di rilascio dell'informativa all'interessato e di acquisizione del consenso dello stesso, nonché dell'eventuale comunicazione a terzi dei dati raccolti;

– società che offrono servizi di cd. *money transfer,* per la verifica delle modalità di informativa all'interessato e di acquisizione del consenso dello stesso, nonché dell'eventuale notificazione del trattamento, delle misure di sicurezza adottate e delle modalità e finalità di raccolta dei dati da fonti terze, con specifico riguardo ai dati personali della clientela;

– società ed enti pubblici che offrono servizi medico-sanitari tramite *app* per *smartphone* o *tablet,* al fine di verificare il rispetto degli obblighi relativi all'informativa e al consenso degli interessati e le modalità adottate al fine di garantire agli stessi l'effettivo esercizio dei diritti di cui agli artt. 7 e ss. del Codice e per la comunicazione dei dati sanitari, nonché la liceità dell'eventuale trattamento di dati relativi alla localizzazione geografica degli interessati o della possibile profilazione degli stessi; sono state inoltre verificate le misure di sicurezza adottate e l'eventuale adempimento degli obblighi di notificazione;

– società che offrono servizi di assicurazione per la responsabilità civile attraverso l'installazione di cd. scatole nere a bordo dei veicoli degli assicurati, al fine di verificare le modalità di trasmissione dei dati dal veicolo alle banche dati utilizzate (interne alla società o esterne in *outsourcing*) e i sistemi di cifratura utilizzati, le modalità dell'eventuale trattamento di geolocalizzazione o profilazione degli interessati ed i connessi adempimenti relativi alla notificazione, al rilascio dell'informativa e alla raccolta del consenso, i soggetti autorizzati all'accesso ai dati raccolti da tali strumenti installati sui mezzi e le relative modalità, le misure di sicurezza adottate e l'eventuale comunicazione di tali dati a terzi;

– agenzie per l'erogazione ed organismi pagatori in agricoltura, con riferimento ai rapporti intercorrenti con i centri di assistenza agricola (c.a.a.) a livello centrale e periferico, per la verifica delle modalità di trattamento dei dati personali degli interessati richiedenti le prestazioni, ivi inclusi gli eventuali controlli sulla corretta adozione delle misure impartite al responsabile ed agli incaricati del trattamento, anche con riferimento ai c.a.a. e alle società ausiliarie convenzionate.

In relazione a quanto emerso dagli accertamenti, effettuati anche nei confronti di singoli titolari del trattamento per esigenze istruttorie connesse a segnalazioni, reclami e ricorsi pervenuti, sono state effettuate numerose proposte di adozione di provvedimenti inibitori e/o prescrittivi per conformare il trattamento alla legge, a fronte delle quali il Garante, come riportato nel prossimo paragrafo, ha adottato alcuni provvedimenti particolarmente significativi.

21.5. *I provvedimenti adottati a seguito dell'attività ispettiva*

In conseguenza dei controlli ispettivi e di connesse penetranti attività istruttorie l'Autorità ha realizzato:

– interventi sui trattamenti illeciti mediante provvedimenti cautelari previsti dalla legge (blocco e divieto) definendo altresì le misure necessarie da prescrivere per rendere il trattamento conforme alla legge (contrasto dell'illecito);

– verifiche sullo stato di attuazione delle prescrizioni adottate dal Garante nei

diversi contesti applicando sanzioni all'esito di accertati inadempimenti al fine di prevenire futuri illeciti (attività preventiva);

– acquisizioni di tutti gli elementi utili a comprendere nuovi fenomeni emergenti che impattano sul diritto alla protezione dei dati personali degli interessati, in modo da definire tempestivamente le misure e gli accorgimenti che devono essere adottati da tutti i soggetti che sono coinvolti nei trattamenti (attività conoscitiva).

Con riferimento all'anno 2018, tra i provvedimenti più rilevanti adottati dal Garante sulla base degli elementi istruttori acquisiti in sede ispettiva si segnalano, in ordine cronologico, i provvedimenti con i quali il Garante ha:

– vietato, ad un operatore di servizi di assistenza telefonica alla clientela e di *customer care* per conto di un rilevante operatore internazionale del settore della televisione a pagamento e dei servizi connessi, l'ulteriore trattamento dei dati personali dei dipendenti attraverso l'utilizzo di un *software* gestionale di tipo CRM (*Custom Relationship Management*) che consentiva, fra l'altro, in assenza di preventiva informativa idonea, il trattamento dei suddetti dati personali su base individuale, con specifico riferimento alla "quantità" e "qualità delle prestazioni lavorative" svolte dai singoli dipendenti; tale sistema, permettendo di ricostruire, anche indirettamente, l'attività effettuata dagli operatori, costituiva uno strumento idoneo a realizzare un controllo a distanza, anche solo potenziale e in via indiretta, dell'attività lavorativa dei dipendenti (provv. 8 marzo 2018, n. 139, doc. web n. 8163433);

– vietato ad uno dei maggiori operatori telefonici nazionali, alla luce degli elementi acquisiti sul trattamento di dati personali mediante il canale telefonico e sulle molteplici operazioni poste in essere per finalità di marketing (tra cui, l'estrazione dei dati riferiti agli interessati dai propri sistemi, l'inserimento degli stessi nelle liste di contattabilità e la successiva trasmissione ai propri *partner* per l'effettuazione dei contatti commerciali) in assenza di un valido consenso degli interessati nonché dei dovuti controlli sull'operato dei propri *partner*; è stato altresì vietato alla suddetta società, in assenza di un'idonea informativa e di un consenso validamente manifestato, l'ulteriore trattamento di dati di profilazione della clientela; infine, è stato prescritto alla stessa l'adozione di misure tecnico-organizzative idonee per valorizzare correttamente nelle proprie liste di esclusione l'eventuale opposizione al trattamento da parte degli interessati e per memorizzare sui propri sistemi informativi i contatti effettuati dai *partner* commerciali nell'interesse della società telefonica (provv. 18 aprile 2018, n. 235, doc. web n. 9358243 – dello stesso tenore, ancorché all'esito di accertamenti ispettivi condotti precedentemente al 2018, v. pure i provv.ti 8 marzo 2018, n. 140, doc. web n. 8233539; 18 aprile 2018, n. 235, doc. web n. 9358243; 22 maggio 2018, n. 313, doc. web n. 8995285);

– accertato l'illiceità del trattamento posto in essere dalle società di un importante gruppo internazionale operante nel settore dei servizi di trasporto automobilistico privato attraverso un'applicazione mobile che mette in collegamento diretto passeggeri e autisti, con riferimento alle informazioni concernenti passeggeri e autisti trattate dal gruppo (per lo più, dati identificativi e di contatto, nonché informazioni concernenti la localizzazione, l'*account* e il numero della patente di guida), in relazione all'inidoneità dell'informativa resa dalle suddette società, alla mancata acquisizione di un valido consenso degli interessati per i dati trattati ai fini dell'individuazione dell'indice di rischio frode, nonché alla mancata notificazione al Garante dei trattamenti di dati idonei a rivelare la posizione geografica degli utenti (provv. 13 dicembre 2018, n. 498, doc. web n. 9069046).

Relativamente ad alcuni dei provvedimenti sopra citati l'Autorità, accertata la violazione di norme del Codice per le quali la legge prevede una sanzione amministrativa, ha avviato anche un procedimento sanzionatorio.

21.6. *L'attività sanzionatoria*

L'attività sanzionatoria del Garante ha registrato molteplici novità nel corso del 2018, che dispiegheranno i loro effetti anche in futuro. Invero, l'applicabilità del RGPD e l'approvazione del decreto legislativo n. 101/2018, hanno profondamente modificato il quadro sanzionatorio in materia di protezione dei dati personali, come meglio illustrato nel successivo par. 21.6.3.

Occorre poi evidenziare che nel 2018, oltre alla consueta attività di accertamento e contestazione delle violazioni, nonché di irrogazione delle relative sanzioni con provvedimenti di ordinanza-ingiunzione, l'Autorità ha dovuto gestire l'attività straordinaria di definizione agevolata dei procedimenti sanzionatori in materia di protezione dei dati personali pendenti alla data del 25 maggio 2018. Al riguardo, l'art. 18 del citato d.lgs. n. 101/2018 ha introdotto la facoltà per i trasgressori, in deroga all'art. 16, l. 24 novembre 1981, n. 689, di definire in via agevolata, mediante il pagamento in misura ridotta di una somma pari a due quinti del minimo edittale, i procedimenti sanzionatori riguardanti le violazioni di cui agli artt. 161, 162, 162-*bis*, 162-*ter*, 163, 164, 164-*bis*, comma 2 e agli artt. 33 e 162, comma 2-*bis,* che non risultassero, alla data di applicazione del RGPD, già definiti con l'adozione dell'ordinanza-ingiunzione.

Vediamo quindi, di seguito, il dettaglio delle attività conseguite nel corso dell'anno 2018.

21.6.1. Violazioni penali e procedimenti relativi alle misure minime di sicurezza

Nell'anno 2018, in relazione alle istruttorie effettuate, sono state inviate n. 27 segnalazioni di violazioni penali all'autorità giudiziaria (cfr. sez. IV, tab. 7), di cui:

– quattordici per la mancata adozione delle misure minime di sicurezza;

– sette per violazioni della legge n. 300/1970 (Statuto dei lavoratori), punite come reato dall'art. 171 del Codice;

– due in relazione ad altre violazioni penali;

– due per inosservanza di un provvedimento del Garante;

– una per trattamento illecito dei dati;

– una in relazione a falsità nelle dichiarazioni al Garante.

Come dimostrano i dati sopra riportati, anche nel 2018 si sono registrate numerose violazioni delle misure minime di sicurezza; ciò nonostante si trattasse di adempimenti di non particolare complessità, in vigore da più di dieci anni. Tuttavia, occorre evidenziare che il decreto legislativo n. 101/2018, conformemente all'impostazione generale del RGPD, ha soppresso, a partire dal 19 settembre 2018, gli obblighi previsti dal Codice (specificatamente dal disciplinare tecnico sulle misure di sicurezza di cui all'All. B al Codice) sull'adozione delle misure minime di sicurezza da parte dei titolari del trattamento.

Sotto il profilo procedurale, nel caso in cui sia rilevata una violazione di una o più delle misure minime di sicurezza, in base al pregresso disposto dell'art. 169, comma 2, del Codice, il Garante ha impartito una prescrizione alla persona individuata come responsabile della predetta violazione e, successivamente, previa verifica del ripristino delle misure violate, ha ammesso il destinatario della prescrizione al pagamento del quarto del massimo della sanzione prevista (pari a 30.000 euro). Gli adempimenti alle prescrizioni ed il pagamento delle somme sono stati comunicati all'autorità giudiziaria competente per le valutazioni in ordine all'estinzione del reato.

Per altro verso, anche nel 2018 si è avuta un'incidenza non trascurabile (7 casi su 27 totali) dell'accertamento di violazioni penali relative allo Statuto dei lavoratori.

Occorre rammentare che la disciplina prevista dallo Statuto e relativa all'utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4) e al divieto di indagini sulle opinioni ai fini dell'assunzione (art. 8), costituisce parte integrante delle disposizioni del Codice (artt. 113 e 114) ed è sanzionata dall'art. 171. Nel rinviare alla trattazione espressamente dedicata alla materia (cfr. par. 13), sul punto basta qui evidenziare che tale disciplina ha subito profonde modifiche a seguito dell'adozione del decreto legislativo 14 settembre 2015, n. 151. Le modifiche apportate attengono sia alla parte sostanziale della disciplina del controllo a distanza dei lavoratori (art. 4, l. n. 300/1970) che a quella sanzionatoria (art. 171 del Codice).

Inoltre, il citato decreto legislativo n. 101/2018 ha ulteriormente modificato la disciplina sanzionatoria, che attualmente prevede, all'art. 171 del Codice: "La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge".

21.6.2. Sanzioni amministrative

Nell'anno 2018 sono stati avviati n. 707 nuovi procedimenti sanzionatori amministrativi. I relativi atti di contestazione sono stati adottati sulla base della disciplina prevista dalla l. n. 689/1981, in virtù del relativo rimando operato dal Codice prima dell'entrata in vigore del decreto legislativo n. 101/2018. Tutti i suddetti procedimenti sanzionatori, tra cui anche quelli avviati nella seconda parte dell'anno (quindi successivamente alla data di applicazione del RGPD), hanno riguardato l'accertamento di violazioni delle norme in materia di protezione dei dati personali avvenute prima del 25 maggio 2018, cioè nella piena vigenza del Codice nella sua formulazione precedente alle modifiche introdotte dal decreto legislativo n. 101/2018, sì che, in applicazione del principio *tempus regit actum*, le violazioni sono state contestate secondo la procedura prevista dalla citata l. n. 689/1981 (cfr. sez. IV, tab. 6).

All'accertamento delle violazioni amministrative previste dal Codice poteva procedere:

– il personale dell'Ufficio del Garante addetto all'attività ispettiva a cui, sulla base di quanto previsto dall'art. 156, comma 9, del Codice, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, è attribuita la qualifica di ufficiale o agente di polizia giudiziaria;

– fino al 25 maggio 2018, chiunque rivestisse, nell'esercizio delle proprie funzioni, la qualifica di ufficiale o agente di polizia giudiziaria, in base a quanto previsto dall'art. 13, l. n. 689/1981.

Le 707 violazioni in relazione alle quali sono stati avviati procedimenti sanzionatori nel 2018 hanno riguardato:

– 424 casi di trattamento illecito per violazione delle disposizioni contenute nell'art. 167 (es. trattamento di dati senza il consenso degli interessati; diffusione di dati sui siti internet delle p.a.; comunicazioni elettroniche indesiderate), sanzionati dall'art. 162, comma 2-*bis;*

– 229 casi di omessa o inidonea informativa all'interessato, sanzionati dall'art. 161;

– 17 casi di omessa o incompleta notificazione ai sensi degli artt. 37 e 38, sanzionati dall'art. 163;

– 14 casi di omessa adozione delle misure minime di sicurezza di cui all'art. 33 (es. mancata designazione degli incaricati; violazione delle disposizioni di cui all'All. B al Codice), sanzionati dall'art. 162, comma 2-*bis;*

– 9 casi di omessa informazione o esibizione di documenti al Garante, sanzionati dall'art. 164;

– 5 casi di inosservanza di un provvedimento del Garante, sanzionati dall'art. 162, comma 2-*ter*;

– 4 casi di violazione di disposizioni del Codice in relazione a banche dati di particolare rilevanza o dimensioni, sanzionati dall'art. 164-*bis,* comma 2;

– 4 casi di violazione delle modalità di comunicazione all'interessato di dati idonei a rivelare lo stato di salute (previste dall'art. 84, comma 1), sanzionati dall'art. 162, comma 2;

– 1 caso di violazione del diritto di opposizione, di cui all'art. 130, comma 3-*bis,* sanzionato dall'art. 162, comma 2-*quater*.

I procedimenti sanzionatori definiti nell'anno 2018 con provvedimento di ordinanza-ingiunzione adottato dall'Autorità, relativamente a violazioni contestate (anche) negli anni precedenti al 2018 stesso e non definite all'epoca attraverso il pagamento spontaneo in misura ridotta da parte del contravventore, sono stati 439. Di questi, 419 hanno comportato l'applicazione di una sanzione (per un ammontare complessivo di somme ingiunte pari a 9.562.600 euro) e 20 si sono invece conclusi con l'archiviazione in quanto la parte ha potuto dimostrare nel procedimento di non aver commesso la violazione contestata o che la violazione non era ad essa imputabile.

È opportuno evidenziare che, in aggiunta ai procedimenti sopra descritti, sono stati definiti ulteriori n. 88 procedimenti sanzionatori attraverso l'esercizio, da parte dei trasgressori, della facoltà di definizione agevolata prevista dal citato art. 18, d.lgs. n. 101/2018 ed il versamento dei relativi importi.

Relativamente alle sopra citate ordinanze-ingiunzione adottate dall'Autorità, invece, appare necessario evidenziare alcuni significativi provvedimenti, tra cui si segnalano, per la particolare rilevanza economica e per il considerevole numero di interessati coinvolti, n. 5 ordinanze-ingiunzioni emesse dal Garante nei confronti di altrettante compagnie telefoniche (consultabili ai docc. web nn. 7665804, 9370122, 9025351, 9040267 e 9079005), con riferimento, in particolare, all'esercizio di attività di marketing non sorrette da idoneo consenso, indirizzate verso clienti ed *ex* clienti (cfr. al riguardo par. 10.2). Nelle predette ordinanze sono stati presi in considerazione, quali elementi determinanti per la quantificazione delle sanzioni, la circostanza che l'utilizzo di molteplici canali di contatto (telefonate su rete fissa, su rete mobile e messaggi *sms*) avesse reso maggiormente invasivo l'illecito trattamento, nonché l'adozione, ancor prima dell'intervento dell'Autorità, di procedure idonee a ricondurre i trattamenti in una cornice di liceità.

In un'altra ordinanza-ingiunzione (provv. 16 maggio 2018, n. 297, doc. web n. 9370122), adottata sempre nei confronti di una compagnia telefonica, il Garante, muovendo dalla segnalazione di un abbonato che lamentava l'indebita intestazione, a suo nome, di un elevato numero di linee telefoniche di rete fissa dallo stesso mai richieste, ha censurato, in termini di maggiore onerosità della sanzione, la circostanza che la compagnia non si fosse attivata con tempestività per risolvere le gravi problematiche segnalate dall'interessato, costringendolo a rivolgersi al Garante.

In tutti i provvedimenti sopra richiamati il Garante, a seguito di un'analisi sulla struttura dei bilanci e sulla posizione nel mercato nazionale e internazionale di ciascuna compagnia, ha applicato l'incremento sanzionatorio previsto in relazione alle rilevanti condizioni economiche dei contravventori. Le società coinvolte hanno versato le sanzioni comminate dal Garante.

Un altro settore significativo è quello relativo all'adozione di n. 22 ordinanze-ingiunzioni nei confronti di altrettanti medici di base di Roma (provv. 22 maggio 2018, n. 335, doc. web n. 9027240) i quali, alla fine del 2014, hanno consentito l'accesso al sistema informativo ai propri sostituti che hanno utilizzato le credenziali di autenticazione dei titolari. Nei provvedimenti del Garante è stato confermato che

i medici titolari hanno l'onere di prevedere accessi separati ai propri applicativi nel caso in cui gli stessi siano utilizzati dai propri sostituti, e che gli accessi di questi ultimi al sistema di monitoraggio della spesa sanitaria debbano avvenire con l'utilizzo di proprie credenziali.

Il Garante ha inoltre adottato un provvedimento sanzionatorio in applicazione delle disposizioni di cui agli artt. 24 e 25, d.lgs. n. 101/2018, che prevede l'irrogazione di sanzioni amministrative in luogo delle sanzioni penali per reati depenalizzati in materia di omessa adozione di misure minime di sicurezza e falsità nelle notificazioni. In un altro caso il Garante, rilevando che l'applicazione della sanzione amministrativa in luogo di quella penale avrebbe determinato una violazione del principio del *ne bis in idem*, ha prospettato l'archiviazione del relativo procedimento.

In materia di telemarketing si segnalano due ordinanze ingiunzioni (provv.ti 31 maggio 2018, n. 368, doc. web n. 9038227 e n. 369, doc. web n. 9038386) adottate dall'Autorità nei confronti di due società che, in qualità di co-titolari, hanno effettuato attività di telemarketing nei confronti di un numero rilevante di soggetti, in violazione delle disposizioni in materia di protezione dei dati personali. In particolare, le società, in modo promiscuo e senza alcuna compartimentazione, hanno raccolto i dati personali degli interessati attraverso tre diversi canali: mediante un *form online*, presente sul sito internet di una delle due società, dagli elenchi telefonici pubblici e, infine, da liste di numerazioni ottenute da una società terza. Tali operazioni di raccolta dati sono state effettuate rendendo agli interessati che accedevano al sito internet un'informativa inidonea e acquisendo un unico consenso a fronte di diverse finalità perseguite; omettendo di acquisire il consenso informato degli interessati le cui numerazioni erano state reperite dalla società terza e, infine, omettendo di verificare presso il Registro pubblico delle opposizioni le numerazioni ottenute dagli elenchi pubblici. Entrambe le società sono state destinatarie di un provvedimento di divieto e prescrittivo (provv. 15 giugno 2017, n. 268, doc. web n. 6629169), nonché delle sanzioni amministrative previste per la violazione degli artt. 13, 23, 130, commi 3 e 3-*bis*, del Codice. È stata altresì applicata la sanzione amministrativa prevista dall'art. 164-*bis*, comma 2, del Codice, che punisce la violazione di un'unica o di più disposizioni indicate nel Capo I del Codice, commesse anche in tempi diversi in relazione a banche dati di particolare rilevanza o dimensioni, con la sanzione amministrativa da euro cinquantamila a euro trecentomila, in considerazione del rilevantissimo numero di dati personali contenuti nella banca dati (circa 1.000.000 di numerazioni). Come più volte ribadito sia dalla giurisprudenza di merito che da quella di legittimità, la fattispecie di cui all'art. 164-*bis,* comma 2, del Codice è del tutto autonoma e distinta rispetto alle fattispecie in essa richiamate. Di qui la configurabilità del cumulo materiale, conseguente all'astratta ipotizzabilità del concorso (non formale) degli illeciti amministrativi tra le fattispecie di cui agli artt. 161 e 162, comma 2-*bis*, in rapporto a quella di cui all'art. 164-*bis*, comma 2, del Codice, quando le prime violazioni (tra le tante possibili secondo il tenore della disposizione esaminata) siano commesse con riferimento a una banca dati di particolare rilevanza e dimensioni.

Il Garante ha adottato un'ordinanza ingiunzione (provv. 22 febbraio 2018, n. 108, doc. web n. 9023215) nei confronti di una impresa individuale per aver effettuato un trattamento di dati personali per mezzo di un sistema di videosorveglianza omettendo di rendere l'informativa agli interessati ai sensi dell'art. 13 del Codice, conservando le immagini per un periodo di tempo superiore a 7 giorni, in violazione di quanto previsto dal Garante nel provvedimento generale sulla videosorveglianza, e, infine, omettendo di adottare le misure di sicurezza ex art. 33 del Codice. Rispetto a tale ultima violazione, essendo stata inoltrata comunicazione di notizia di reato all'autorità giudiziaria, è stata sollevata, in sede difensiva, la possibile configu-

rabilità dell'istituto della connessione per pregiudizialità ex art. 24, l. n. 689/1981. L'Autorità ha avuto così modo di chiarire che la valutazione circa la ricorrenza dell'istituto della connessione (per pregiudizialità) della violazione amministrativa con un reato (nel caso di specie, quella dell'art. 33 del Codice), di cui all'art. 24, l. n. 689/1981, è rimessa esclusivamente all'autorità giudiziaria procedente. Che tali valutazioni siano di competenza dell'autorità giudiziaria e che precedano la fase della contestazione, si ricava dall'art. 14, comma 3, della medesima legge, in base alla quale, quando la connessione non sussiste, l'autorità giudiziaria dispone "con provvedimento" la trasmissione degli atti all'"Autorità competente" per la contestazione della violazione amministrativa e quindi l'avvio del procedimento sanzionatorio. Nella fattispecie in esame, avendo il Pubblico ministero autorizzato l'utilizzo ai fini amministrativi degli elementi acquisiti in ambito penale, per la contestazione della violazione amministrativa, emerge la piena competenza del Garante a definire il relativo procedimento sanzionatorio.

In riferimento all'utilizzo di dispositivi finalizzati alla localizzazione di persone ed oggetti, il Garante, nel sanzionare una società esercente l'attività di *car sharing* per la mancata indicazione, nel testo dell'informativa da rilasciare ai clienti, di riferimenti alla finalità e alle modalità riguardanti la funzione di geolocalizzazione dei veicoli a noleggio, ha definito il concetto di localizzazione "continuativa" di cui al provvedimento recante "Chiarimenti sui trattamenti da notificare al Garante - 23 aprile 2004" (doc. web n. 993385), nonché al provvedimento concernente sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro del 4 ottobre 2011 (doc. web n. 1850581). Ha ritenuto, infatti, sussistente il requisito della "continuità" qualora la posizione del mezzo sia rilevabile a discrezione del titolare del trattamento, ossia ogniqualvolta il titolare del trattamento sia in grado di conoscere, in qualsiasi momento, automaticamente o meno (anche, ad es., attraverso un meccanismo conoscitivo come una telefonata o l'invio di un *sms*) la posizione del conducente sul veicolo geolocalizzato, prescindendo quindi dalla staticità o dinamicità del sistema di localizzazione e/o dalla possibilità o meno di una tracciatura costante in via automatica di tutto il percorso effettuato dal veicolo geolocalizzato (provv. 15 febbraio 2018, n. 86, doc. web n. 8990236).

21.6.3. Versamenti relativi alle sanzioni amministrative

Il decreto legislativo n. 101/2018 ha introdotto talune importanti novità anche in relazione alla "Definizione agevolata delle violazioni in materia di protezione dei dati personali", a decorrere dal 19 settembre 2018. Si rende necessario, pertanto, al fine di illustrare i versamenti riscossi nell'anno 2018 a titolo di sanzione amministrativa, effettuare una breve premessa in merito alla situazione riguardante i procedimenti sanzionatori oggetto della definizione agevolata.

L'art. 18, d.lgs. n. 101/2018 ha introdotto la possibilità di definire in maniera agevolata taluni procedimenti sanzionatori (riguardanti le violazioni degli artt. 161, 162, 162-*bis*, 162-*ter*, 163, 164, 164-*bis*, comma 2, 33 e 162, comma 2-*bis*, del Codice) che, alla data del 25 maggio 2018, non risultino ancora definiti mediante l'adozione di ordinanza-ingiunzione.

Alla data di entrata in vigore del predetto decreto, rientravano nell'ambito di applicazione dello stesso circa n. 1.688 procedimenti sanzionatori, per un totale complessivo di importi contestati pari a € 26.955.734. In relazione a tali procedimenti sanzionatori era quindi ammesso il pagamento in misura ridotta, entro novanta giorni dalla data di entrata in vigore del decreto legislativo n. 101/2018 (pertanto, entro il 18 dicembre 2018) di una somma pari a due quinti del minimo edittale. L'introito previsto dalla definizione agevolata, nell'ipotesi in cui avessero

aderito tutti coloro che rientravano nei presupposti contenuti nel citato decreto, era pari a 5.798.400 euro.

In realtà, la suddetta procedura di definizione agevolata ha registrato una bassa adesione da parte dei soggetti coinvolti, conducendo alla definizione di n. 88 procedimenti sanzionatori ed alla conseguente riscossione di un importo totale pari a € 386.400.

Ciò ha comportato che, nel corso dell'anno 2019, per effetto delle previsioni di cui al citato art. 18, d.lgs. n. 101/2018, saranno automaticamente iscritte a ruolo le sanzioni già contestate, senza necessità di ulteriori provvedimenti, per tutti i procedimenti sanzionatori per i quali non siano state presentate nuove memorie difensive entro il 16 febbraio 2019 (cfr. art. 18, comma 2).

Fatta questa necessaria premessa, si rileva che l'ammontare dei pagamenti effettivamente riscossi nell'anno 2018 da parte dei soggetti nei cui confronti sono stati avviati procedimenti sanzionatori amministrativi è risultato complessivamente pari a 8.161.806 euro (cfr. sez. IV, tab. 8) di cui:

– 1.305.600 euro, pagati a titolo di definizione in via breve;

– 5.362.262 euro, a seguito di ordinanze-ingiunzione adottate dal Garante in tutti i casi in cui la parte non si è avvalsa della facoltà di definizione in via breve di cui al punto precedente;

– 90.000 euro, per la definizione, in sede amministrativa, dei procedimenti penali relativi alla mancata adozione delle misure minime di sicurezza;

– 1.017.544 euro, quali ulteriori entrate derivanti dall'attività sanzionatoria (es. riscossione coattiva);

– 386.400 euro, a titolo di versamenti spontanei per la definizione agevolata dei procedimenti sanzionatori pendenti alla data del 25 maggio 2018, di cui all'art. 18, d.lgs. n. 101/2018.

Si evidenzia, in particolare, il significativo incremento, rispetto all'anno precedente, dei versamenti spontanei effettuati a fronte delle sanzioni irrogate con ordinanza-ingiunzione (passati da € 1.329.590 nel 2017 a € 5.362.262 nel 2018). Tale risultato è ascrivibile alla frequente acquiescenza prestata dai contravventori ai provvedimenti di ordinanza-ingiunzione adottati dal Garante, tra cui, in particolare, quelli nei confronti dei quattro maggiori operatori telefonici nazionali (provv. 18 gennaio 2018, n. 16, doc. web n. 7665804; provv. 16 maggio 2018, n. 297, doc. web n. 9370122; provv. 22 maggio 2018, n. 330, doc. web n. 9018431; provv. 5 luglio 2018, n. 412, doc. web n. 9025351; provv. 26 luglio 2018, n. 441, doc. web n. 9040267; provv. 29 novembre 2018, n. 493, doc. web n. 9079005), che hanno condotto all'irrogazione di sanzioni per un importo complessivamente pari a € 4.400.000, di cui sono stati versati, nel 2018, € 3.800.000 (i residui € 600.000 saranno versati nel 2019).

Gli importi relativi alle sanzioni applicate dal Garante sono versati sul bilancio dello Stato. Sulla base di quanto previsto dall'art. 166 del Codice, tali proventi, nella misura del 50% del totale annuo sono riassegnati al fondo stanziato per le spese di funzionamento dell'Autorità previsto dall'art. 156, comma 8, del Codice, per essere destinati alle specifiche attività di sensibilizzazione e di ispezione nonché di attuazione del RGPD svolte dal Garante.

21.7. *Il nuovo quadro sanzionatorio introdotto dal RGPD*

La complessa riforma della normativa in materia di protezione dati si fonda su vari componenti: la coerenza del quadro normativo, la semplificazione delle proce-

dure, il coordinamento degli interventi, il coinvolgimento degli utenti, le strategie informative più efficaci e il rafforzamento dei poteri di attuazione.

Un requisito essenziale ai fini dell'armonizzazione del nuovo quadro normativo è costituito dall'attuazione coerente del nuovo assetto: le sanzioni amministrative pecuniarie rappresentano un elemento centrale nel nuovo regime introdotto dal RGPD e un potente strumento con il quale le autorità di controllo possono attuare la normativa unitamente alle altre misure correttive.

Una volta accertata la violazione del RGPD, dopo aver valutato i fatti del caso, il Garante deve individuare le "misure correttive" più appropriate per affrontare tale violazione.

Le disposizioni di cui all'art. 58, par. 2, lett. da *b*) a *j*), del RGPD, indicano gli strumenti che le autorità di controllo hanno a disposizione per far fronte a un'inadempienza da parte di un titolare o responsabile del trattamento.

In particolare, sono previste sanzioni: fino a dieci milioni di euro o, per le imprese, fino al 2% del fatturato per la violazione degli obblighi del titolare e del responsabile, dell'organismo di certificazione o dell'organismo di controllo; fino a venti milioni di euro o, per le imprese, fino al 4% del fatturato per la violazione dei princìpi di base del trattamento (artt. 5, 6 7 e 9), dei diritti degli interessati (artt. Da 12 a 22), degli obblighi previsti dagli Stati nelle materie del capo IX (artt. da 85 a 91 – es. giornalismo, lavoro, ricerca scientifica, storica, statistica, segreto professionale), in caso di trasferimento di dati personali al di fuori dell'Unione europea (artt. da 44 a 49); in caso di inosservanza di un ordine o di una limitazione del Garante o di diniego all'accesso ai dati e ai locali (art. 58, par. 1 e 2).

L'articolo 15, d.lgs. n. 101/2018 ha poi modificato l'art. 166 del Codice, disponendo, sulla base della facoltà concessa agli Stati membri dall'art. 84 del RGPD, di introdurre nuove sanzioni per le violazioni non sanzionate dal Regolamento stesso, che sono configurabili ulteriori illeciti amministrativi in corrispondenza della violazione delle disposizioni del Codice (sono state così introdotte dieci ulteriori fattispecie sanzionate ai sensi dell'art. 83, par. 4, del RGPD e più di cinquanta ulteriori fattispecie sanzionate ai sensi dell'art. 83, par. 5, del RGPD).

A titolo meramente esemplificativo, si applica la sanzione amministrativa pecuniaria fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per:

– la violazione, da parte del titolare, dell'obbligo di redigere con linguaggio particolarmente chiaro e semplice, comprensibile e accessibile al minore, le informazioni e le comunicazioni relative al trattamento che lo riguardi (in relazione all'offerta diretta di servizi della società dell'informazione) (art. 2-*quinquies*, comma 2, del Codice);

– la violazione delle misure introdotte dal Garante con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che può presentare rischi particolarmente elevati ai sensi dell'art. 35 del RGPD (art. 2-*quinquiesdecies* del Codice).

Sempre a titolo di esempio, si applica la sanzione amministrativa pecuniaria fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per:

– la violazione delle disposizioni relative alla comunicazione e diffusione di dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 2-*ter* del Codice);

– la violazione delle norme sul trattamento di particolari categorie di dati personali per motivi di interesse pubblico rilevanti (2-*sexies* del Codice);

– la diffusione in dati genetici, biometrici e relativi alla salute (art. 2-*septies*, comma 8, del Codice);

– la violazione delle norme sul trattamento dei dati relativi a condanne penali (art. 2-*octies,* del Codice);

– la violazione della disciplina sul trattamento dei dati sanitari (art. 75 del Codice).

Per quanto riguarda gli illeciti penali, il RGPD non interviene ma consente agli Stati di introdurre "altre sanzioni" (cfr. art. 84).

Anche in questo caso il decreto legislativo n. 101/2018, nel perimetro di intervento delineato dalla legge delega n. 163/2017, ha realizzato una riforma del quadro sanzionatorio penale, modificando alcuni illeciti vigenti e introducendone di nuovi (artt. 167 e seguenti del Codice novellato).

In particolare, a titolo meramente esemplificativo, viene sanzionato penalmente, salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto o di arrecare danno all'interessato:

– violi gli artt. 123 (dati relativi al traffico), 126 (dati relativi all'ubicazione) e 130 (comunicazioni indesiderate) o il provvedimento di cui all'art. 129 (contraenti in elenchi) e arrechi nocumento all'interessato, con la reclusione da sei mesi a un anno e sei mesi;

– tratti dati personali di cui agli artt. 9 (dati particolari) e 10 (condanne penali e reati) del RGPD in violazione degli artt. 2-*sexies* (dati particolari per pubblico interesse) e 2-*octies* (dati relativi a condanne penali e reati), o delle misure di garanzia ad esso relative ovvero operando in violazione delle misure adottate e arrechi nocumento all'interessato, con la reclusione da uno a tre anni;

– trasferisca dati personali verso un Paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli artt. 45, 46 o 49 del RGPD e arrechi nocumento all'interessato, con la reclusione da uno a tre anni.

Inoltre, è penalmente rilevante anche la condotta di chiunque, al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, acquisisca con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, ovvero comunichi o diffonda tale archivio senza il consenso degli interessati (ove necessario) oppure in violazione degli artt. 2-*ter* (base giuridica), 2-*sexies* (dati particolari per pubblico interesse) e 2-*octies* (dati relativi a condanne penali e reati).

Infine, come ricordato in precedenza, è prevista la sanzione penale della reclusione anche per chi, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiari o attesti falsamente notizie o circostanze o produca atti o documenti falsi, o comunque, in generale, cagioni intenzionalmente un'interruzione o turbi la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

Una volta accertata una violazione del RGPD sulla base di una valutazione dei fatti nel caso di specie, l'autorità di controllo competente deve individuare le misure correttive più idonee al fine di gestire tale violazione. Le disposizioni contenute nell'art. 58, par. 2, del RGPD individuano gli strumenti che le autorità possono utilizzare in caso di violazioni commesse da un titolare o da un responsabile del trattamento.

Nell'esercitare tali poteri, le autorità di controllo devono osservare taluni principi fondamentali avendo cura di individuare una misura correttiva "effettiva, proporzionata e dissuasiva". Analogamente a ogni altra misura correttiva, anche le sanzioni amministrative pecuniarie dovrebbero corrispondere adeguatamente alla natura, alla gravità e alle conseguenze della specifica violazione: le autorità di controllo devono

valutare tutte le circostanze del caso di specie secondo un approccio coerente e basato su criteri oggettivi. Nel valutare quanto sia effettivo, proporzionato e dissuasivo nel singolo caso, occorre anche tenere conto dell'obiettivo perseguito attraverso la misura correttiva volta per volta individuata – ossia, ristabilire l'osservanza della norma, ovvero punire la condotta illecita (o l'uno e l'altro di tali obiettivi).

Il RGPD prevede che ogni caso sia oggetto di una valutazione individuale. Il punto di partenza ai fini di tale valutazione individuale è rappresentato dall'art. 83, par. 2, disposizione secondo la quale "Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi: …". Pertanto, anche alla luce del considerando 148, spetta all'autorità di controllo individuare la misura o le misure più idonee. Nei casi di cui all'art. 83, paragrafi da 4 a 6, tale operazione deve prendere in considerazione la totalità delle misure correttive, compresa l'imposizione dell'idonea sanzione amministrativa pecuniaria in associazione a una misura correttiva di cui all'art. 58, paragrafo 2, ovvero in forma isolata.

21.7.1. I criteri di valutazione fissati all'art. 83, par. 2, del RGPD

L'art. 83, par. 2, del RGPD contiene un elenco di criteri che le autorità di controllo devono utilizzare per valutare se irrogare una sanzione pecuniaria e, in caso affermativo, per stabilirne l'importo. Ciò non significa che sia necessario ripetere la valutazione utilizzando gli stessi criteri, bensì che nella valutazione occorre tener conto di tutte le circostanze di ogni singolo caso come prevede lo stesso art. 83. Le conclusioni raggiunte nella prima fase della valutazione possono essere utilizzate nella seconda fase relativa alla definizione dell'importo della sanzione pecuniaria, in tal modo evitando la necessità di ripetere la valutazione sulla base degli stessi criteri.

La quasi totalità degli obblighi incombenti su titolari e responsabili del trattamento ai sensi del RGPD è classificata in base alla rispettiva natura nelle disposizioni contenute ai par. da 4 a 6 dell'art. 83. Nel fissare due diversi importi massimi della sanzione amministrativa pecuniaria (rispettivamente, 10 e 20 milioni di euro), il RGPD segnala già che una violazione di certe disposizioni si configura come più grave rispetto alla violazione di altre disposizioni. Tuttavia, l'autorità di controllo competente, nel valutare le circostanze del caso di specie alla luce dei criteri generali fissati nell'art. 83, par. 2, può decidere che, nel caso specifico, sussiste una maggiore o minore necessità di rispondere con una misura correttiva sotto forma di sanzione pecuniaria. Qualora si decida di ricorrere alla sanzione pecuniaria quale misura correttiva, isolatamente ovvero congiuntamente ad altre misure correttive, si applicherà il sistema classificatorio del RGPD (art. 83, par. da 4 a 6) al fine di individuare la sanzione pecuniaria massima irrogabile in base alla natura della specifica violazione.

Il considerando 148 introduce il concetto di "violazioni minori". Si tratta di violazioni che possono riguardare una o più fra le disposizioni del RGPD di cui all'art. 83, par. 4 o 5. Tuttavia, la valutazione dei criteri al par. 2 dell'art. 83 può far ritenere all'autorità di controllo che, alla luce delle circostanze concrete del caso di specie, la violazione, per esempio, non comporta un rischio significativo per i diritti degli interessati né inficia l'essenza dell'obbligo in oggetto. In casi del genere, alla sanzione può sostituirsi un ammonimento. Al riguardo, infatti, il considerando 148, non configura alcun obbligo per l'autorità di controllo di sostituire l'ammonimento alla sanzione amministrativa pecuniaria ogniqualvolta abbia a che fare con una violazione minore "potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria"; si tratta, semmai, di una possibilità cui fare ricorso in base alla concreta valutazione di tutte le circostanze del caso di specie.

Il medesimo considerando 148, peraltro, indica la possibilità di rivolgere un

ammonimento anziché imporre una sanzione pecuniaria qualora il titolare sia una persona fisica e la sanzione pecuniaria verosimilmente comminabile costituisca un onere sproporzionato. Il punto di partenza dell'analisi è la necessità per l'autorità di controllo di valutare se, alla luce delle circostanze del caso specifico, debba imporre una sanzione amministrativa pecuniaria. Se l'autorità decide a favore di quest'ultima, dovrà anche valutare se la sanzione pecuniaria ipotizzata costituisca un onere sproporzionato per la persona fisica e, in tal caso, rivolgendo un ammonimento (cfr. in merito Gruppo Art. 29, WP 253, Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679, adottate il 3 ottobre 2017, p. 9).

Il RGPD non attribuisce un importo specifico alle specifiche violazioni, bensì fissa unicamente un importo massimo. Tale importo può segnalare una gravità relativamente minore per le violazioni degli obblighi di cui al par. 4 dell'art. 83 rispetto agli obblighi di cui al par. 5 di tale articolo. Tuttavia, l'effettività, proporzionalità e dissuasività della risposta individuata in caso di violazione delle disposizioni di cui all'art. 83, par. 5, dipenderanno dalle circostanze del singolo caso.

22 Le relazioni comunitarie e internazionali

22.1. *La cooperazione tra le autorità di protezione dati nell'UE: dal Gruppo Art. 29 al Comitato europeo per la protezione dati*

Cessazione del Gruppo Art. 29 e insediamento del CEPD

Nei primi mesi del 2018, il Gruppo Art. 29 (Gruppo) ha proseguito i lavori sui temi legati all'applicazione del RGPD, per favorire il processo di adeguamento al nuovo quadro normativo e dare piena attuazione allo stesso. Come già ricordato, il RGPD è divenuto, infatti, pienamente applicabile a decorrere dal 25 maggio 2018, data in cui si è tenuta la prima riunione del Comitato europeo per la protezione dei dati (*European Data Protection Board*, d'ora in poi CEPD o Comitato) preceduta dalla cessazione dell'attività del Gruppo, che per oltre vent'anni ha svolto un'intensa e preziosa attività di coordinamento e supporto del lavoro delle autorità di protezione dati dei 28 Paesi membri.

Il CEPD che, a differenza del Gruppo, è un vero e proprio organismo europeo dotato di personalità giuridica, è composto, ai sensi dell'art. 68 del RGPD, dalle autorità nazionali di controllo dei singoli Stati membri e dal Garante europeo per la protezione dei dati (GEPD) e si riunisce con la partecipazione, senza diritto di voto, della Commissione europea. Alle riunioni del Comitato partecipano anche le autorità di controllo dei tre Paesi parti dell'Accordo sullo spazio economico europeo (Norvegia, Liechtenstein e Islanda), con gli stessi diritti e obblighi delle autorità di controllo degli Stati membri dell'UE, fatta eccezione per il diritto di voto e il diritto di candidarsi alle cariche di presidente e di vicepresidenti (decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018 che ha modificato l'Accordo SEE al fine di integrarvi il RGPD).

Il CEPD, presieduto da Andrea Jelinek (già presidente del Gruppo Art. 29), si è riunito cinque volte nel 2018. Nel corso della sua prima riunione, il Comitato ha adottato le proprie regole procedurali (RoP) – che disciplinano, tra l'altro, la procedura di adozione di pareri e decisioni ai sensi degli artt. 64, 65 e 66 del RGPD – e un *Memorandum of Understanding* per regolare i rapporti con il Garante europeo per la protezione dei dati, chiamato a svolgere la funzione di Segretariato per il Comitato stesso. Per garantire e sottolineare la continuità dei lavori rispetto al passato, il Comitato ha inoltre formalmente approvato (*endorsement*) tutte le Linee guida del Gruppo in relazione alle novità introdotte dal RGPD, ivi comprese quelle adottate dallo stesso, in via preliminare o a seguito di consultazione pubblica, nel corso dei primi mesi del 2018 (le notizie relative alle attività del Comitato, le Linee guida e tutti i documenti sono rinvenibili al sito internet: https://edpb.europa.eu).

Linee guida in materia di decisioni automatizzate e profilazione

Tra queste, le Linee guida in materia di decisioni automatizzate e profilazione (WP 251), le quali, pur riconoscendone i possibili vantaggi in termini di efficienza e risparmio di risorse, sottolineano i rischi significativi che da tali trattamenti possono derivare sui diritti delle persone, segnatamente in termini di discriminazione, stigmatizzazione e negazione di beni e servizi, e forniscono indicazioni in ordine alle nuove disposizioni introdotte dal Regolamento in materia. Le Linee guida si soffermano, in particolare, sulla definizione di "profilazione" e forniscono criteri interpretativi riguardo al regime delle "decisioni basate unicamente sul trattamento automa-

tizzato, che producono effetti giuridici sulla persona o incidono in modo significativo su di essa e sui diritti specifici degli interessati" previsti dall'art. 22 del RGPD (cfr. Relazione 2017, p. 159).

Linee guida in materia di notifica delle violazioni di dati personali

Sempre a seguito degli esiti di una consultazione pubblica, sono state riviste ed adottate le Linee guida in materia di notifica delle violazioni di dati personali (WP 250, rev. 01). Il documento (di cui si è dato conto anche nella Relazione 2017, p. 160) chiarisce gli obblighi di notifica e di comunicazione delle violazioni sanciti dal RGPD e le misure che i titolari e i responsabili del trattamento devono intraprendere per ottemperare a tali nuovi obblighi, fornendo alcuni esempi di violazioni e dei casi in cui la notifica deve essere inviata all'autorità di protezione dei dati e agli interessati.

Linee guida in materia di trasparenza

Parallelamente, il Gruppo ha adottato in via definitiva le Linee guida in materia di trasparenza, modificate alla luce dei commenti degli *stakeholder* che hanno partecipato alla consultazione pubblica (WP 260, rev. 01, Relazione 2017, p. 160). Il documento sottolinea la valenza fondamentale dell'obbligo di trasparenza gravante sui titolari e fornisce una guida interpretativa sui requisiti previsti dagli artt. 12 - 14 del RGPD, con particolare riguardo agli aspetti pratici dell'adempimento (tempistica dell'informativa, strumenti per fornire la stessa, etc.). Il documento reca anche una scheda riassuntiva degli obblighi del titolare in materia di trasparenza.

Linee guida in materia di consenso

Il Gruppo ha altresì adottato in via definitiva le nuove Linee guida sul consenso (WP 259, rev. 01, Relazione 2017, p. 159), anche in questo caso tenendo conto dei risultati della consultazione pubblica a cui hanno partecipato numerosi *stakeholder* (soprattutto dei settori marketing, ricerca, ambito finanziario e assicurativo). Partendo dal precedente parere 15/2011, il documento fornisce un'analisi approfondita della nozione di consenso, segnalandone i punti di novità alla luce del RGPD e fornendo chiarimenti sui requisiti per ottenere (e comprovare) il consenso valido dell'interessato. Il consenso rimane una delle basi giuridiche per trattare i dati personali (art. 6 del RGPD) e, per quanto riguarda l'attuale direttiva 2002/58/CE relativa alla tutela della vita privata nelle comunicazioni elettroniche, il Gruppo rileva che i requisiti per il consenso ai sensi del RGPD non sono da considerare un "obbligo supplementare", ma condizioni preliminari per la liceità del trattamento (art. 95 del RGPD).

I registri delle attività di trattamento e le PMI

Negli ultimi mesi di attività il Gruppo ha adottato il *Position paper* relativo all'art. 30, par. 5, del RGPD sui registri delle attività di trattamento per le piccole e medie imprese (PMI). Il documento spiega che le PMI che impiegano meno di 250 persone sono esentate dal mantenimento di tale registro per le sole attività che non siano tra quelle previste dall'art. 30, par. 5 (ossia quelle relative a trattamenti che possano presentare un rischio per i diritti e le libertà dell'interessato, a trattamenti non occasionali o a trattamenti di particolari categorie di dati personali, incluse condanne penali o reati). Il documento chiarisce che è sufficiente che l'impresa esegua anche uno solo di tali trattamenti per aversi l'obbligo di istituire il registro, il quale può tuttavia essere limitato a questi ultimi (e non contenere quindi le eventuali diverse tipologie di trattamenti effettuati dall'impresa). Infine, il documento, sottolineando l'importanza del registro come strumento utile all'analisi delle implicazioni dei trattamenti di dati avviati o pianificati all'interno di un'impresa, incoraggia le autorità di protezione dati a supportare le PMI fornendo loro strumenti per facilitare la predisposizione e il mantenimento di tale registro (ad es., tramite modelli semplificati di registro da pubblicare *online*).

Linee guida sull'accreditamento degli organismi di certificazione

Prima di cessare il proprio mandato, il Gruppo ha adottato e avviato la consultazione pubblica sulle Linee guida in materia di accreditamento degli organismi di certificazione (WP 261), che mirano a fornire indicazioni sull'interpretazione e l'attuazione delle disposizioni di cui all'art. 43 del RGPD, al fine di stabilire un quadro

di riferimento coerente e armonizzato per l'accreditamento degli organismi che rilasciano certificazioni in conformità al RGPD. Il documento illustra le procedure disponibili per l'accreditamento degli organismi di certificazione a norma dell'art. 43, par. 1, e fornisce indicazioni in ordine ai requisiti di accreditamento che le autorità di protezione dei dati devono stabilire, in aggiunta a quelli previsti dalla norma ISO/IEC 17065/20122, quando l'accreditamento è gestito dall'organismo nazionale di accreditamento. Il documento contiene inoltre un quadro di riferimento per le autorità di protezione dei dati che devono fissare i requisiti di accreditamento da seguire laddove il legislatore nazionale lasci alle stesse il compito di accreditare direttamente gli organismi di certificazione. Tali Linee guida sono state adottate in via definitiva, dopo consultazione pubblica, a dicembre 2018. Alle stesse è aggiunto un allegato volto a fornire indicazioni su come definire i requisiti aggiuntivi di accreditamento a partire da quanto previsto dall'art. 43, par. 2, del RGPD e dalla norma ISO/IEC 17065/2012.

Linee guida in materia di certificazione

Sempre in tema di certificazioni, al fine di fornire indicazioni comuni minime agli Stati membri e alle stesse autorità di supervisione per un'applicazione omogenea delle pertinenti disposizioni del Regolamento, sono state adottate dal Comitato le Linee guida sulle certificazioni e sui criteri di certificazione ai sensi degli artt. 42 e 43 del RGPD. Il documento, sottoposto a consultazione pubblica in vista dell'adozione definitiva avvenuta il 23 gennaio 2019 (Linee guida n. 1/2018), si sofferma sull'apporto delle certificazioni quali strumenti per dimostrare l'*accountability* di titolari e responsabili del trattamento e sui concetti chiave contenuti nelle due disposizioni; chiarisce il ruolo delle autorità di protezione dei dati nell'adozione dei criteri di certificazione (e del Comitato in relazione al sigillo europeo per la protezione dei dati), le quali possono, ma non hanno l'obbligo, di agire come certificatori, nonché il loro possibile ruolo nel rilasciare le certificazioni stesse. Da ultimo, le Linee guida chiariscono che il *focus* delle certificazioni deve essere basato sulla *compliance* dei trattamenti effettuati dai titolari e responsabili e che non possono essere certificati quindi Rpd.

Linee guida sull'ambito di applicazione territoriale del RGPD

A novembre 2018, il Comitato ha adottato e sottoposto a consultazione pubblica le Linee guida relative all'ambito di applicazione territoriale del RGPD (Linee guida n. 3/2018), fornendo indicazioni in merito all'interpretazione dell'art. 3 del RGPD, tanto nel caso in cui venga in rilievo l'art. 3, par. 1 (criterio dello stabilimento sul territorio dell'Unione europea) o l'art. 3, par. 2 (criterio del *targeting*), quanto nell'eventualità dell'applicazione dell'art. 3, par. 3 (criterio del luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico). Le Linee guida forniscono diversi esempi, soffermandosi sulla nozione di stabilimento e sul criterio del *targeting*. Le stesse si esprimono anche in merito al ruolo e alle responsabilità dei rappresentanti di titolari o di responsabili del trattamento non stabiliti nell'Unione cui si applichi la disciplina ai sensi dell'art. 3, par. 2, del RGPD, in particolare in relazione all'*enforcement* in caso di mancata osservanza degli obblighi del Regolamento da parte dei titolari o dei responsabili che rappresentano.

Elenchi delle tipologie di trattamenti soggetti alla valutazione d'impatto sulla protezione dei dati

Il Comitato ha espresso, nel corso del 2018, il proprio parere su ciascuna delle liste con cui ventisei autorità di protezione dati hanno individuato i trattamenti che devono essere sottoposti a valutazione di impatto ai sensi dell'art. 35 del RGPD poiché presentano un rischio elevato per i diritti e le libertà delle persone fisiche e possono avere un impatto in più di uno Stato membro. Tali elenchi costituiscono uno strumento rilevante per l'applicazione coerente del RGPD, fermo restando che resta in capo a ciascun titolare del trattamento stabilire, alla luce del caso concreto, se una valutazione d'impatto sia necessaria prima di avviare l'attività di trattamento. A parere del Comitato, tali liste devono presentare almeno due criteri di rischio per

ciascuna tipologia di trattamento e contenere un "nucleo comune" obbligatorio di tipologie di trattamenti; tra essi, in particolare, i pareri individuano i trattamenti che hanno ad oggetto dati genetici, biometrici e di localizzazione. Il Comitato, richiamando le Linee guida in materia di valutazione d'impatto sulla protezione dei dati (WP 248, rev. 01, adottato nell'ottobre 2017: v. Relazione 2017, pp. 158 e 159), ha chiarito, tra l'altro, che non possono essere considerati quali criteri di rischio una specifica base giuridica o il trattamento ulteriore dei dati e che le liste non devono contenere una definizione numerica o percentuale del concetto di "larga scala".

Codici di condotta

Il Comitato ha avviato i lavori per la predisposizione di linee guida in materia di codici di condotta partendo anche dall'esperienza acquisita nella valutazione dei progetti di codici sottoposti alla sua attenzione nel corso del 2018. Diversi aspetti sono stati oggetto di discussione, fra i quali la natura e il ruolo dei promotori, il meccanismo di monitoraggio e l'accreditamento dell'organismo di monitoraggio.

La necessità di approfondire la natura e il ruolo dei promotori dei codici è stata evidenziata in occasione della predisposizione di una lettera inviata ai promotori del codice di condotta per le applicazioni mobili nel settore della salute, su una cui precedente bozza il Gruppo Art. 29 si era già espresso nel 2017 (cfr. Relazione 2017, p. 163). A seguito della presentazione di una nuova versione della bozza di codice di condotta priva di sostanziali cambiamenti rispetto alla proposta originaria, il Comitato ha chiesto ai promotori di rivederlo e, nell'ottica di una possibile sua futura presentazione quale codice di condotta ai sensi dell'art. 40 del RGPD, di fornire maggiori informazioni in ordine alla forma giuridica del "consorzio" che lo ha elaborato.

Sempre in materia di codici di condotta, il Gruppo ha inoltre fornito indicazioni in merito al progetto del codice di condotta *Cloud Infrastructure Providers in Europe* (CISPE) presentato dall'associazione europea dei fornitori di infrastrutture *cloud*. Con la nota, il Gruppo ha espresso una valutazione positiva sull'iniziativa, accompagnata però da alcuni rilievi volti, tra l'altro, a richiedere l'introduzione di previsioni più specifiche in ordine ai trattamenti che il codice di condotta intende coprire, alle responsabilità del fornitore di servizi di infrastruttura *cloud* e in materia di sicurezza.

Trasferimento dati all'estero

In materia di trasferimento di dati all'estero, il Gruppo ha adottato, a seguito di consultazione pubblica, la versione definitiva del documento in materia di adeguatezza – che indica i requisiti generali e i principi fondamentali e procedurali affinché un Paese terzo o un'organizzazione internazionale possano essere considerati "adeguati" ai sensi dell'art. 45 RGPD (WP 254, cfr. Relazione 2017, p. 167) – e dei due *referential* relativi alle Norme vincolanti di impresa (*Binding Corporate Rules*, di seguito Bcr) per titolari e per responsabili (WP 256 e 257: cfr. Relazione 2017, p. 167). I due documenti illustrano gli elementi che le Bcr devono contenere per poter essere considerate, alla stregua del RGPD, garanzie adeguate per il trasferimento dei dati in Paesi terzi. Tali garanzie specificano e integrano quelle espressamente previste dall'art. 47 del RGPD il quale, innovando rispetto alla direttiva 95/46/CE, riconosce espressamente le Bcr quale strumento idoneo per il trasferimento dei dati fuori dall'UE.

A corredo dell'approvazione dei due nuovi *referential* per le Bcr, il Gruppo ha anche aggiornato i modelli per la presentazione delle Bcr per titolari (WP 264) e per responsabili (WP 265). I modelli – che devono essere utilizzati da tutte le società che intendono richiedere l'approvazione delle proprie Bcr – riflettono le modifiche più rilevanti apportate con il RGPD in relazione, tra l'altro, ai diritti del terzo beneficiario e alle loro modalità di esercizio, ai principi di protezione dei dati, alla obbligatoria responsabilità in capo ad una delle società del gruppo stabilite nell'Unione;

nei modelli è contenuta anche una nuova sezione relativa alle misure volte a soddisfare il requisito dell'*accountability* e dei principi di *privacy by design* e *by default*.

Il Gruppo ha poi adottato un documento di lavoro sulla procedura di approvazione delle Bcr (WP 263 rev. 01), volto ad aggiornare il precedente documento in materia (WP 107). Sulla scorta dell'esperienza maturata, il documento fornisce indicazioni in ordine ai criteri per l'identificazione dell'autorità competente per l'approvazione delle norme vincolanti d'impresa (cd. Bcr *lead*), richiamando sostanzialmente i medesimi criteri già individuati nel precedente WP 107, e definisce la procedura di cooperazione da seguire prima della presentazione della bozza definitiva al Comitato per il parere richiesto dall'art. 64, par. 1, lett. *f*), del RGPD. In sintesi, il documento prevede che la Bcr *lead* interagisca con il gruppo imprenditoriale e con le altre autorità interessate (fungendo sostanzialmente da punto di contatto), presenti la bozza di decisione per l'approvazione delle Bcr al Comitato e adotti poi, alla luce del parere ottenuto, la decisione finale sulle Bcr ai sensi dell'art. 64, par. 7, del RGPD. Le Bcr così approvate saranno considerate come "garanzie adeguate" anche negli altri Paesi UE, dove potranno essere utilizzate dall'impresa senza autorizzazione specifica (art. 46, par. 2, lett. *b*), del RGPD). Questa nuova procedura di cooperazione è già stata avviata in relazione a diverse richieste di approvazione di Bcr, ma nessuna richiesta di parere ai sensi dell'art. 64, par. 1, lett. *f*), è stata proposta dinanzi al Comitato nel 2018.

A seguito di consultazione pubblica, sono state adottate in via definitiva dal Comitato anche le Linee guida (n. 2/2018) in materia di deroghe per il trasferimento dei dati all'estero di cui all'art. 49 del RGPD. Il documento fornisce una serie di orientamenti in merito all'utilizzo delle deroghe relative al trasferimento di dati personali verso Paesi terzi e contiene una ricognizione casistica varia. Anzitutto, chiarisce cosa si intende per trasferimento occasionale, ossia un trasferimento che avvenga non con cadenza regolare e in circostanze non ordinarie, ad esempio al manifestarsi di condizioni casuali o ignote e a intervalli di tempo arbitrari. Viene altresì specificato quando il consenso – esplicito, informato e specifico rispetto ai possibili rischi del trasferimento – possa essere considerato un valido fondamento giuridico per il trasferimento dati verso paesi terzi. Il documento chiarisce inoltre che, affinché un trasferimento possa essere effettuato sulla base della deroga del rilevante interesse pubblico, tale interesse deve essere riconosciuto nell'Unione e può anche essere riconducibile a trattati o accordi internazionali di cui un Paese è parte. Le Linee guida si soffermano anche sulla nuova previsione dell'art. 49, par. 1, lett. *g*), del RGPD, relativa alla possibilità di considerare il legittimo interesse quale base giuridica per il trasferimento dei dati all'estero, richiamando l'attenzione dell'esportatore sulle particolari condizioni e precauzioni che caratterizzano il possibile utilizzo di tale deroga.

Il 5 dicembre 2018 è stato adottato il parere sulla proposta di decisione di adeguatezza nei confronti del Giappone presentata dalla Commissione europea (n. 28/2018). Il parere del Comitato raccomanda alla Commissione di chiarire alcuni importanti aspetti. In particolare, si sofferma sulla necessità di monitorare con attenzione la vincolatività delle cd. disposizioni supplementari adottate dall'Autorità di protezione dei dati giapponese su delega del Governo al fine di adeguare la propria normativa al RGPD. Posto che tali disposizioni supplementari si applicheranno solo ai dati provenienti dall'Unione, il Comitato ha chiesto alla Commissione di verificare che tale specifica tutela sia garantita fino alla loro cancellazione (anche attraverso modalità che consentano alle imprese di identificare la provenienza del dato personale in questione). Il parere chiede inoltre di chiarire meglio la figura del cd. *trustee*, incardinata nella normativa giapponese, la quale, pur somigliando a

quella del responsabile del trattamento ai sensi dell'art. 28 del RGPD, non appare corrispondere del tutto a quest'ultima. Profili di criticità sono stati evidenziati in ordine alle garanzie in occasione di trasferimenti ulteriori di dati personali provenienti dall'UE a Paesi terzi (cd. *onward transfers*): l'eventuale decisione di adeguatezza adottata dall'Autorità giapponese nei confronti di Paesi terzi, che consentirebbe il trasferimento ulteriore di questi dati verso di essi, non terrebbe infatti conto delle regole supplementari, prima citate, negoziate con la Commissione UE. Più in generale, con riferimento a questo e agli altri aspetti ritenuti più critici, il parere raccomanda di monitorare l'effettiva applicazione del nuovo quadro giuridico creato per i dati provenienti dall'UE. La Commissione europea ha tenuto conto dei rilievi del Comitato, modificando la proposta inziale con riferimento ai profili così rilevati, e ha adottato la decisione di adeguatezza del Giappone il 23 gennaio 2019.

A seguito della seconda revisione annuale del *Privacy shield* (l'accordo negoziato nel 2016 fra Unione europea e Stati Uniti per il trasferimento dati verso le società certificate nel quadro dello stesso: cfr. Relazione 2016, p. 153), il CEPD – che ha partecipato alla revisione con sei suoi rappresentanti – ha adottato, a gennaio 2019, il secondo *report* sulla sua applicazione. Esso sottolinea alcuni progressi sia in relazione agli aspetti commerciali (quali, ad es., i maggiori controlli nella prima fase di certificazione delle imprese e l'adozione di linee guida per individui e imprese), sia in relazione agli aspetti concernenti l'accesso ai dati da parte di autorità pubbliche per finalità di *law enforcement* e sicurezza (in particolare, la nomina dei membri necessari per il funzionamento del *Privacy and Civil Liberties Oversight Board* - PCLOB e una maggiore trasparenza in relazione alle attività di *intelligence*).

Il documento individua, tuttavia, alcuni aspetti sui quali è auspicabile un'ulteriore attività volta ad un'applicazione più puntuale dell'accordo: per la parte commerciale, maggiore attenzione alla verifica sostanziale del rispetto dei principi dell'accordo e chiarimenti in ordine alla loro interpretazione, in particolare con riferimento ai trattamenti dei dati relativi alle risorse umane, alle garanzie per i trasferimenti ulteriori e ai trattamenti effettuati dai responsabili del trattamento; per la parte relativa ai trattamenti effettuati per finalità di *law enforcement* e sicurezza, il parere invita il PCLOB a produrre ulteriori *report* in ordine all'applicazione della legislazione di riferimento (PPD-28, *Executive Order* 12333 e la sezione 702 del FISA) e sottolinea come ancora, anche in ragione della mancata declassificazione di molti documenti, il Comitato non sia in grado di ritenere l'*Ombudsperson* (che peraltro ancora non è stato designato in via definitiva) quale effettivo rimedio giudiziario in linea con l'art. 47 della Carta dei diritti fondamentali dell'UE.

Protezione dei dati e attività finanziaria

Il Garante ha continuato a coordinare il sottogruppo *Financial matters* incaricato, prima nell'ambito del Gruppo Art. 29 e poi del Comitato, di approfondire le diverse questioni legate all'applicazione della disciplina sulla protezione dei dati nel settore finanziario.

In tale ambito è proseguito il lavoro sullo scambio di informazioni tra autorità di controllo dei mercati finanziari, in particolare in relazione ai meccanismi da porre in essere affinché i trasferimenti di dati dalle autorità finanziarie europee alle loro omologhe extra UE siano effettuati nel rispetto dei principi di protezione dati. In base all'art. 46, par. 3, lett. *b*) del RGPD, autorità pubbliche o organismi pubblici possono stipulare accordi amministrativi, comprensivi di diritti effettivi e azionabili per gli interessati, per assicurare le garanzie necessarie a legittimare i trasferimenti di dati verso Paesi terzi non adeguati. Il Comitato ha esaminato la bozza di accordo predisposta dall'Autorità europea degli strumenti finanziari e dei mercati (ESMA) insieme all'Organizzazione internazionale delle commissioni sui valori mobiliari (IOSCO) e, all'esito di un intenso e proficuo confronto, la stessa è stata in buona

parte modificata. Il Comitato ha adottato, il 12 febbraio 2019, il parere richiesto ai sensi dell'art 64, par. 2, del RGPD (parere 4/2019), concludendo che la versione finale dell'accordo assicura le garanzie adeguate necessarie ai trasferimenti di dati in Paesi terzi e fornendo alcune indicazioni riguardo all'implementazione dei meccanismi di tutela posti in essere dall'accordo stesso.

In ambito finanziario è altresì proseguita l'attività del Comitato relativa alle analisi delle implicazioni della normativa statunitense FATCA (*Foreign Account Tax Compliance Act*) sulla tutela della vita privata e sul principio di non discriminazione, previsti dagli artt. 8 e 14 della Convenzione europea dei diritti dell'uomo. L'8 febbraio 2018, il Gruppo Art. 29 ha adottato una lettera di riscontro alla petizione presentata al Parlamento europeo e portata all'attenzione della Presidente del Gruppo sulle implicazioni di FATCA, in particolare con riferimento agli effetti di tale normativa sui cd. *accidental Americans* (persone che non hanno legami effettivi con gli USA ma la sola cittadinanza sulla base dello *ius soli*) e a coloro che hanno la doppia cittadinanza UE/USA, i cui dati sono comunque obbligatoriamente trasmessi dalle autorità fiscali europee a quelle statunitensi.

È stato altresì portato avanti il lavoro di analisi del rapporto tra il RGPD e la direttiva (UE) 2015/2366 sui servizi di pagamento (cd. PSD2), due normative chiave della legislazione europea degli ultimi anni. La direttiva PSD2 consente a nuovi soggetti di attuare servizi che un tempo erano prerogativa esclusiva delle banche, consentendo ad essi di accedere ad una mole considerevole di dati finanziari non solo dei clienti, ma anche di terzi (ad es., i beneficiari di ordini di pagamento). Il sottogruppo ha evidenziato come la direttiva deve essere interpretata nel pieno rispetto dei principi del RGPD, peraltro espressamente richiamato dalla stessa PSD2.

In risposta a una lettera indirizzata dall'europarlamentare Sophie in't Veld, il Comitato, in data 5 luglio 2018, ha fornito prime indicazioni su alcuni punti controversi del rapporto tra PSD2 e RGPD, in particolare con riferimento alla natura del consenso esplicito richiamato dall'art. 94 della PSD2 e alla tutela delle cd. *silent third parties,* i cui dati sono oggetto di trattamento da parte dei fornitori di servizi di pagamento in quanto, come ricordato, beneficiari di ordini di pagamento. In tale occasione il Comitato ha sottolineato l'importanza di attivare una proficua interazione tra le autorità finanziarie competenti a livello europeo e le autorità di protezione dei dati al fine di instaurare un approccio coordinato che fornisca maggiori tutele per le persone.

Protezione dei dati e *law enforcement*

Con l'adozione del parere sull'interoperabilità tra i sistemi informativi (attuali e futuri) nell'ambito di dogane, immigrazione, protezione internazionale e cooperazione in ambito di polizia e giudiziaria (WP 266 del 18 aprile 2018), il Gruppo Art. 29 si è espresso sulle proposte di regolamento della Commissione in materia (COM 2017/793 e COM 2017/794). Il progetto riguarda le banche dati di SIS II, VIS, EURODAC, il futuro *Entry-exit-system* (EES) e – in caso di adozione – il futuro *European Travel Information and Authorisation System* (ETIAS), nonché l'*European Criminal Record Informations System for Third Country Nationals* (ECRIS-TCN). Il parere sottolinea le criticità delle proposte regolamentari in ordine alla necessità e proporzionalità delle misure previste e si sofferma su alcuni aspetti specifici legati al possibile futuro funzionamento del sistema, quali la conservazione dei dati, il sistema di supervisione e le misure di sicurezza.

A seguito del parere della CGUE del 26 luglio 2017 (parere 1/15) sul progetto relativo al nuovo Accordo tra l'Unione europea e il Canada sull'uso dei dati del codice di prenotazione (PNR), è stata inviata una lettera alla Commissione europea con la quale il Gruppo Art. 29 ha richiamato l'attenzione sulla necessità di rivedere anche gli accordi PNR già siglati con l'Australia e con gli Stati Uniti d'America,

nonché la stessa direttiva (UE) 2016/681 sul PNR europeo. Alcune previsioni di tali documenti, infatti, coincidono con quelle oggetto di censura da parte della Corte. In particolare, il Gruppo richiama l'attenzione sulla necessità di identificare più chiaramente negli accordi la tipologia dei dati oggetto di trasferimento, di valutare la liceità del trattamento di dati sensibili e le condizioni che consentono la conservazione e l'accesso ai dati PNR dopo che l'interessato ha passato i controlli di frontiera.

Il Gruppo ha fornito inoltre il proprio parere alla Commissione per le libertà civili, la giustizia e gli affari interni (LIBE) del Parlamento europeo, in merito alle conseguenze della "riautorizzazione" della sezione 702 del *Foreign Intelligence Surveillance Act* (FISA) da parte del Presidente degli Stati Uniti. Nella propria comunicazione il Gruppo ha fornito elementi in ordine alle modifiche apportate dalla "riautorizzazione" e ha precisato che le stesse, volte a prevedere un ordine giudiziario per l'accesso alle comunicazioni in determinate circostanze, per quanto apprezzabili, sembrerebbero applicabili solo ai cittadini statunitensi.

Prendendo avvio dalle considerazioni già svolte nella dichiarazione del novembre 2017 sul tema (Relazione 2017, p. 165), il Comitato ha adottato il parere n. 23/2018 sulle proposte della Commissione relative agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018) 225 final) e alle norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali (COM(2018) 226 *final*), che contengono le regole e le procedure che le autorità giudiziarie dovranno seguire per poter richiedere "le prove elettroniche" direttamente ai *service provider* di altri Paesi. Il parere del Comitato si sofferma sugli aspetti più preoccupanti delle proposte e, tra essi, la base giuridica nella proposta di regolamento sulle prove elettroniche (al momento identificata nell'art. 82, par. 1, del TFUE, il quale riguarda, però, la cooperazione tra autorità giudiziarie), la necessità e la proporzionalità della proposta – in particolare alla luce della presenza di altri strumenti per l'acquisizione transfrontaliera delle prove come la Convenzione sulla criminalità informatica (cd. Convenzione di Budapest), i *Mutual Legal Assistance Treaty* (MLAT) e la direttiva relativa all'ordine europeo di indagine penale (direttiva 2014/41/UE) –, l'abbandono di principi fondamentali (ad es., il requisito della cd. doppia punibilità e il criterio di ubicazione dei dati, secondo cui questi devono essere richiesti nel luogo ove siano effettivamente conservati).

Protezione dei dati e nuove tecnologie

In materia di crittografia, il Gruppo ha adottato uno *statement* in cui si sottolinea la necessità dell'adozione di una crittografia "forte" per garantire un flusso di dati sicuro e libero tra individui, imprese e governi. In particolare, il documento ha evidenziato come le *backdoors* e le chiavi principali privino la crittografia della sua utilità e non possano essere utilizzate in modo sicuro, atteso che non esiste un modo sicuro per implementare tali tecniche. Il Gruppo ha pure segnalato la possibilità per le forze dell'ordine di utilizzare – per l'accesso ai dati necessari ad indagare e perseguire la criminalità – strumenti già disponibili, quali un numero di *gateway* legali e strumenti mirati.

Proposta di regolamento *e-Privacy*

Alla luce dell'importanza accordata dal Comitato ad una rapida conclusione della revisione della direttiva *e-Privacy* (2002/58/CE), è stato adottato lo *statement* sulla proposta di regolamento in materia di riservatezza nelle comunicazioni elettroniche, con cui si enfatizza l'opportunità di un regolamento specifico in materia, segnatamente per soddisfare il bisogno di una tutela della confidenzialità delle comunicazioni elettroniche che non abbassi il livello di protezione offerto dall'attuale direttiva *e-Privacy*. In particolare, nel documento si sottolinea la necessità che il consenso dell'interessato sia ottenuto sistematicamente, con modalità tecnica-

mente fattibili e prima del trattamento dei dati o prima di utilizzare le capacità di archiviazione o di elaborazione dell'apparecchiatura terminale dell'utente, escludendo che il "legittimo interesse" o il fine generico dell'esecuzione di un contratto possano rappresentare eccezioni alla regola del consenso. Si auspica il ricorso a modalità efficaci di raccolta del consenso da parte dei siti web e delle applicazioni mobili, anche mediante l'utilizzo di impostazioni che preservino la *privacy* degli utenti per impostazione predefinita (*by default*), guidando gli stessi alla scelta delle impostazioni in maniera efficace e trasparente. Si chiarisce inoltre che, ai fini della raccolta di un consenso libero al trattamento dei dati personali, l'accesso ai servizi e alle funzionalità non deve essere subordinato a tale consenso e, pertanto, il trattamento delle informazioni connesse alle apparecchiature terminali degli utenti finali, ossia i *cookie wall*, devono essere espressamente proibiti. Lo *statement* incentiva il ricorso ad un'effettiva anonimizzazione dei dati relativi alle comunicazioni elettroniche e sottolinea la necessità di un approccio neutrale dal punto di vista tecnologico in relazione a tutti i tipi di comunicazioni elettroniche, compresi quelli effettuati dai servizi cd. *over-the-top* (OTT). In merito alle eventuali eccezioni che i legislatori nazionali potrebbero prevedere in aggiunta a quelle già individuate nella proposta, il documento invita ad un'attenta disamina delle stesse, anche al fine di scongiurare il monitoraggio indiscriminato dell'ubicazione dell'utente o il trattamento dei metadati riferiti allo stesso, con particolare riguardo alle richieste di accesso da parte di autorità pubbliche.

ICANN

Il Gruppo ha inoltre proseguito la sua attività di approfondimento sulle questioni relative al trattamento dei dati nell'ambito dell'*Internet Corporation for Assigned Names and Numbers* (ICANN) – l'ente *no profit* che gestisce il sistema dei nomi a dominio di primo livello – in particolare con riferimento ai principi di protezione dei dati che devono applicarsi al cd. registro *Whois*, sul quale ICANN sta lavorando da tempo per ridefinire le proprie regole. Sul tema il Gruppo si era già pronunciato con lettera del dicembre 2017 (cfr. Relazione 2017, p. 163) e a seguito di questa, ICANN ha pubblicato un documento (*Proposed Interim Model for GDPR Compliance*) che prevede un approccio multilivello secondo cui solo alcuni dati rimarrebbero pubblici, mentre la maggior parte di essi sarebbe accessibile solo da terze parti accreditate.

Con una lettera inviata nel mese di aprile 2018, il Gruppo ha preso atto delle maggiori garanzie introdotte con il nuovo modello, pur evidenziando alcune persistenti criticità, quali la necessità di una chiara individuazione delle finalità e delle rispettive condizioni di liceità, di un consenso libero quando lo stesso costituisce la base giuridica prescelta, di regole chiare per l'accesso ai dati non pubblici, nonché quelle concernenti la sicurezza, i termini di conservazione dei dati e i trasferimenti di dati all'estero.

Il Comitato si è poi nuovamente occupato del trattamento dei dati personali effettuato in ambito ICANN, adottando una dichiarazione nella quale si esclude una moratoria per i titolari del trattamento, consapevoli da tempo della necessità di adeguarsi alle regole del RGPD. Infine, con una lettera del 5 luglio 2018, il Comitato ha invitato ICANN a sviluppare un modello di *Whois* che permetta l'uso dei dati da parte di soggetti legittimati (comprese le autorità di *law enforcement*) nel rispetto del regolamento e senza che ciò porti ad una pubblicazione illimitata dei dati.

Protezione dei dati e *e-Health*

Il tema *e-Health* è stato affrontato dal Gruppo in occasione dell'invio alla Commissione europea di una lettera relativa all'Accordo per lo scambio di dati sanitari in attuazione della direttiva 2011/24/UE sull'assistenza sanitaria transfrontaliera (il cui obiettivo è la promozione di una cooperazione tra la Commissione e gli Stati

membri per l'elaborazione di misure volte a favorire l'interoperabilità dei rispettivi sistemi sanitari elettronici nazionali e agevolare così l'accesso transfrontaliero dei pazienti alle applicazioni di assistenza sanitaria *online*). Il documento affronta i principali aspetti per i quali risultano alcune criticità o che necessitano di ulteriori approfondimenti, in particolare in relazione alla base giuridica per lo scambio elettronico transfrontaliero di dati sanitari tra gli Stati membri partecipanti all'Accordo e alla natura e struttura dell'Accordo e dei suoi allegati. La lettera sottolinea inoltre la necessità di provvedere ad una valutazione di impatto sulla protezione dati e di una attenta valutazione in ordine ai periodi di conservazione dei dati, alla trasparenza nei confronti degli interessati e agli eventuali trattamenti ulteriori.

22.2. *La cooperazione delle autorità di protezione dati nel settore libertà, giustizia e affari interni*

Europol cooperation board

In virtù del nuovo quadro normativo creato dal regolamento (UE) 2016/794, entrato in vigore il 1° maggio 2017, la supervisione sull'attività svolta dall'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) è svolta dal GEPD. Rimane di competenza delle autorità nazionali di protezione dei dati la vigilanza della legittimità della comunicazione di dati ad Europol da parte delle autorità di *law enforcement* e la verifica circa il rispetto dei diritti degli interessati. Al fine di assicurare una stretta cooperazione tra il GEPD e le autorità nazionali è stato istituito, con funzioni consultive, un Consiglio di cooperazione (*Europol Cooperation Board*) che nel 2018 si è riunito due volte, il 30 maggio e il 3 ottobre.

Durante la prima riunione, il Consiglio è stato informato circa gli esiti delle attività ispettive condotte presso Europol e, in particolare, della prima svolta direttamente dal GEPD nell'esercizio delle nuove funzioni ispettive (in passato le attività ispettive sono state effettuate dall'autorità comune di controllo Europol che ha cessato le proprie funzioni ad aprile 2017: v. Relazione 2017, p. 168) alla quale hanno partecipato, in qualità di esperti, anche rappresentanti di autorità nazionali (tra cui quella italiana).

Il Consiglio ha adottato il programma di lavoro per il periodo 2018-20 che, tra l'altro, prevede di facilitare l'esercizio dei diritti dell'interessato, collaborare con la Commissione per la revisione degli accordi di cooperazione per il trasferimento di dati da parte di Europol verso Paesi terzi, verificare il rispetto delle regole sul trattamento dei dati di minori, seguire le iniziative legislative della Commissione sulla interconnessione tramite interoperabilità dei sistemi informativi su larga scala nei settori del controllo delle frontiere, asilo, immigrazione, cooperazione di polizia e giudiziaria in materia penale.

Per consentire agli interessati l'esercizio dei loro diritti, il Gruppo ha invitato i componenti ad aggiornare la lista delle autorità, distinguendo chiaramente tra i dati di contatto dell'autorità nazionale competente per l'esercizio del diritto di accesso a Europol e i dati di contatto dell'autorità nazionale di protezione dei dati. Ciò in qualche caso ha comportato una messa a punto delle competenze in materia di accesso.

È stata esaminata con grande attenzione l'eventualità di utilizzare il sistema SIENA (*Secure Information Exchange Network Application*) per lo scambio di informazioni non relative all'ambito di competenze stabilito per Europol, giungendo alla conclusione che è necessario attenersi a quanto stabilito dal regolamento (UE) 2016/794 e segnatamente dal suo allegato II, che individua le categorie di dati personali e le categorie di interessati i cui dati possono essere raccolti e trattati ai fini

dei controlli incrociati relativi ai reati oggetto dell'ambito di competenza di Europol.

Attenzione è stata dedicata anche agli strumenti che facilitano lo scambio di informazioni tra le autorità nazionali di *law enforcement* dei diversi Paesi e, in particolare, sul possibile utilizzo del sistema *European Tracking Solution* (ETS), uno strumento che consentirebbe ad unità specializzate di scambiare dati sulla posizione geografica quasi in tempo reale.

Nel corso delle riunioni, si è anche deciso l'aggiornamento dell'opuscolo "Conosci i tuoi diritti", volto a chiarire le modalità per l'esercizio dei diritti di protezione dei dati in relazione ai trattamenti effettuati dall'Agenzia e di un manuale rivolto alle autorità nazionali di *law enforcement* competenti che fornisca indicazioni in ordine ai dati da inviare ad Europol.

Gruppo di coordinamento della supervisione del Sistema informativo Schengen (SIS II)

Il sistema d'informazione Schengen (SIS II) è il sistema d'informazione centralizzato su larga scala che viene utilizzato come strumento d'ausilio per i controlli sulle persone e sugli oggetti alle frontiere esterne dello spazio Schengen. Secondo quanto previsto dal quadro giuridico del SIS II (regolamento CE 1987/2006 e decisione del Consiglio 2007/533/GAI), la supervisione coordinata del sistema è di competenza del Gruppo di coordinamento della supervisione SIS II, di cui fanno parte le autorità di protezione dati dei Paesi membri – che assicurano la supervisione delle autorità nazionali competenti per il sistema SIS II – e il GEPD, incaricato della supervisione del trattamento dati posto in essere dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (Eu-LISA), che gestisce il sistema centrale.

Nel corso del 2018 il Gruppo di coordinamento della supervisione SIS II si è riunito due volte (i documenti sono reperibili presso il sito del Gruppo alla pagina: https://edps.europa.eu/data-protection/european-it-systems/schengen-information-system_en). Nel corso della prima riunione è stata adottata una lettera indirizzata, in data 22 giugno 2018, al Presidente del Parlamento europeo volta ad evidenziare forti preoccupazioni in ordine a due proposte di regolamento presentate dalla Commissione a fine 2017 in materia di interoperabilità dei sistemi informativi (attuali e futuri) nell'ambito di dogane, immigrazione, protezione internazionale e cooperazione in ambito di polizia e giudiziaria (COM 2017/793 e COM 2017/794). Nella lettera, firmata congiuntamente anche dai presidenti dei gruppi di supervisione Eurodac e VIS, le tre autorità sottolineano che la proposta interconnessione dei singoli sistemi – ognuno dei quali creato per finalità specifiche – rischia di ledere i principi di finalità e proporzionalità e necessita di una più attenta valutazione di impatto sui diritti fondamentali degli interessati. Le autorità, nel rifarsi al parere adottato sul tema dal Gruppo l'11 aprile 2018 (WP266), ha richiamato l'attenzione del Parlamento su alcuni aspetti da definire, tra cui la chiara individuazione, da un lato, delle finalità per le quali le autorità di polizia potranno accedere alle informazioni del costituendo "archivio comune di dati di identità" (un nuovo *database* che consentirà di raccogliere tutti i dati della medesima persona contenuti in ciascun sistema) e, dall'altro, della titolarità del trattamento dei nuovi *database*. Il documento si sofferma inoltre sulla necessità di adottare misure di *privacy by design* e *by default* e di introdurre misure specifiche di salvaguardia per i dati relativi a minori, anziani e disabili.

Nella sua seconda riunione (il 14 novembre 2018), il Gruppo ha adottato il rapporto delle attività 2016-2017 e ha discusso del tema delle segnalazioni ai sensi dell'art. 24 della decisione SIS II con l'obiettivo di preparare un documento che si incentri sull'elenco dei criteri utilizzati a livello nazionale per l'inserimento nel sistema di tali segnalazioni. Altre tematiche oggetto di discussione sono state le

future attività di interesse del Gruppo di supervisione per il periodo 2019-2021 al fine di individuare quelle ritenute prioritarie e, nuovamente, il tema del futuro della supervisione con riferimento all'aspetto relativo alla futura composizione dell'organismo di supervisione che, nel dover rispecchiare la composizione di quanti partecipano al sistema SIS II, dovrebbe ricomprendere tanto rappresentanti di Paesi UE che di Paesi non UE (ad es., la Svizzera).

Gruppo di supervisione del sistema Eurodac

Il Gruppo di supervisione del sistema Eurodac (i cui documenti sono rinvenibili sul sito internet alla pagina: https://edps.europa.eu/data-protection/european-it-systems/eurodac_en) è competente per assicurare il rispetto della protezione dei dati personali all'interno del sistema istituito per la comparazione delle impronte digitali dei richiedenti asilo.

Il Gruppo si è riunito due volte nel 2018 (il 13 giugno e il 15 novembre). Nel corso delle riunioni sono stati discussi e poi adottati il rapporto sulle attività svolte dal Gruppo per il periodo 2016-2017 e un questionario volto a raccogliere informazioni su come l'esercizio dei diritti degli interessati sia garantito nei diversi stati membri. Durante la prima riunione è stato anche presentato il rapporto "*Under wacthful eyes - Biometrics, EU IT systems and fundamental rights*" dell'Agenzia europea per i diritti fondamentali, il quale si sofferma sulle implicazioni per i diritti fondamentali nell'impiego di dati, inclusi quelli biometrici, nei sistemi IT dell'UE nei settori dell'asilo e immigrazione, e sottolinea la mancanza di effettività del principio di trasparenza nel trattamento dei dati nei confronti degli interessati (i richiedenti asilo). La Commissione ha inoltre presentato un resoconto sullo stato dei lavori per la revisione del regolamento Eurodac (regolamento n. 603/2013) che prevede, fra l'altro, un'estensione dello scopo di applicazione per identificare i soggiorni irregolari, un abbassamento della soglia di età per la quale le impronte digitali sono acquisite (da 14 anni a 6) e la conservazione delle immagini nel sistema centrale per consentire l'uso di tecnologie per il riconoscimento facciale. Il Gruppo ha deciso di monitorare la revisione del quadro normativo nell'ambito del programma di lavoro 2019-2021, con particolare attenzione ai temi dell'accesso delle autorità di *law enforcement* al sistema; attenzione verrà prestata anche al rispetto del diritto di accesso e alle attività ispettive delle autorità nazionali di protezione dati.

Gruppo di coordinamento della supervisione del Sistema informativo visti (VIS)

Il Gruppo di supervisione VIS è competente per il monitoraggio del sistema d'informazione visti, istituito dalla decisione 2004/512/CE e volto a creare uno spazio di libertà, sicurezza e giustizia senza frontiere interne tramite lo scambio di dati relativi ai visti d'ingresso nello spazio Schengen tra gli Stati che ne fanno parte. Il funzionamento del VIS è disciplinato dal regolamento (CE) 767/2008 e consiste in una banca dati centrale a livello europeo alla quale sono connesse le interfacce nazionali delle autorità degli Stati Schengen competenti per i visti, tra cui gli uffici consolari e i valichi di frontiera esterni degli Stati.

Nel corso del 2018, il Gruppo di supervisione (i cui documenti sono rinvenibili sul sito internet: https://edps.europa.eu/data-protection/european-it-systems/visa-information-system_en) si è riunito due volte.

In occasione della prima riunione (il 13 giugno 2018) è stato adottato un documento sulle regole di protezione dei dati applicabili ai contratti con i cd. *External service providers*, i quali, in particolari circostanze previste dal Codice visti, cooperano con i consolati all'emissione dei visti di breve periodo. Il documento detta alcune raccomandazioni in merito e prevede che tali contratti contengano, tra l'altro, una clausola che consenta all'autorità di protezione dati di monitorare l'attività del fornitore di servizio in questione, le modalità per l'accesso ai dati da parte degli interessati e il limite temporale per la loro cancellazione.

Nel corso della seconda riunione (15 novembre 2018) è stato discusso e adottato

il documento relativo alla posizione del Gruppo in merito alla proposta presentata dalla Commissione il 16 maggio 2018 (COM(2018) 302 *final*) volta ad emendare la disciplina di settore. La proposta reca modifiche al codice dei visti (regolamento (CE) 810/2009), al regolamento che istituisce un sistema di ingressi/uscite per la registrazione dei dati relativi al respingimento dei cittadini di Paesi terzi che attraversano le frontiere (regolamento (UE) 2017/2226), al codice frontiere Schengen (regolamento (UE) 2016/399) e, alla luce anche della prevista futura interoperabilità dei sistemi e delle nuove regole che dovranno disciplinarla, prevede l'abrogazione della decisione 2008/633/GAI relativa all'accesso al VIS da parte delle autorità di *law enforcement*. Nel proprio documento, il Gruppo, nel ribadire l'importanza del necessario rispetto delle specifiche finalità del VIS, ha evidenziato alcuni aspetti critici e tra questi, in particolare, la previsione dell'accesso al sistema da parte delle autorità di polizia per attività tipiche delle forze dell'ordine. Analoghe perplessità sono state espresse in relazione al previsto accesso a tali dati da parte dell'agenzia Europol.

Il Gruppo ha poi affrontato il tema della formazione in materia di sicurezza e protezione dei dati del personale delle autorità che hanno accesso al sistema, adottando un questionario relativo alla metodologia utilizzata per garantirla e ha incontrato, come nei precedenti anni, il responsabile della protezione dei dati dell'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (Eu-LISA) che ha fornito alcuni dati acquisiti monitorando il sistema VIS. Il gruppo ha, infine, avviato la discussione sul programma di lavoro per il triennio 2019-2021 e ha condiviso alcune informazioni relative alle consuete valutazioni nazionali sull'*Acquis* Schengen avvenute nel corso dell'anno.

Il Sistema informativo doganale (SID): ACC Dogane e Gruppo di coordinamento della supervisione SID

Il Sistema informativo doganale è volto a consentire la cooperazione tra le autorità nazionali competenti per la prevenzione, la ricerca e il perseguimento di gravi infrazioni delle leggi nazionali in materia (decisione 2009/917/GAI e della decisione quadro 2008/977/GAI) e quelle competenti a contrastarne le violazioni di natura amministrativa (sulla base del regolamento (CE) 515/1997, consolidato nel 2008). Per i trattamenti effettuati in ambito di polizia e giustizia, la supervisione è attribuita all'Autorità comune di controllo dogane (ACC Dogane), mentre per la cooperazione di tipo amministrativo la competenza è attribuita al Gruppo di coordinamento della supervisione del Sistema informativo doganale (sito internet alla pagina: https://edps.europa.eu/data-protection/supervision-coordination/customs-information-systems_en). Mentre l'ACC Dogane non si è riunita nel 2018, nell'attesa della ricostituzione del proprio segretariato, il Gruppo di coordinamento si è riunito due volte, adottando il rapporto delle attività 2016-2017 e continuando il lavoro volto alla predisposizione di una guida comune per le attività di verifica dei sistemi e l'aggiornamento, anche alla luce delle novità introdotte dal RGPD, della guida relativa ai diritti degli interessati, adottata nel 2015 (cfr. Relazione 2015, p. 181).

22.3. *La partecipazione dell'Autorità in seno al Consiglio d'Europa e ad altri gruppi di lavoro internazionali*

Comitato consultivo della Convenzione 108/1981 (T-PD)

È proseguita l'intensa attività del Comitato consultivo (cd. T-PD) della Convenzione del Consiglio d'Europa 108/1981 (Convenzione sulla protezione degli individui rispetto al trattamento automatizzato dei dati personali), la cui presidenza, assunta dalla rappresentante del Garante nel 2016, è stata riconfermata nella plenaria del 19-21 giugno per il secondo mandato.

Convenzione 108+

Il 2018 è stato un anno particolarmente significativo per le attività in materia di protezione dati del Consiglio d'Europa: dopo un lungo *iter* iniziato nel 2011, si è

infatti concluso il processo di modernizzazione della Convenzione 108, con l'adozione, in data 18 maggio 2018, del protocollo emendativo della Convenzione avvenuta in occasione della riunione ministeriale di Elsinore. Il protocollo emendativo (il cui testo è reperibile, insieme a tutti i documenti del T-PD sul sito web: www.coe.int/en/web/data-protection) è stato aperto alla firma delle Parti il 10 ottobre 2018 in occasione della sessione dell'Assemblea Parlamentare del Consiglio d'Europa con la partecipazione di un alto numero di stati firmatari. L'Italia ha provveduto a sottoscrivere il protocollo emendativo in data 5 marzo 2019.

La modernizzazione della Convenzione 108, che è tuttora l'unico strumento sulla protezione dei dati vincolante a livello internazionale, risponde alle molte sfide intervenute negli anni a seguito dello sviluppo delle nuove tecnologie e della globalizzazione, assicurando la tenuta dei principi della Convenzione nel nuovo scenario e rafforzando i meccanismi per la sua effettiva implementazione. Come l'originaria Convenzione, il protocollo garantisce standard elevati di protezione in una cornice normativa flessibile che facilita la loro adozione da parte di un ampio numero di Paesi, inclusi quelli che non fanno parte del Consiglio d'Europa e ai quali il protocollo è aperto; esso costituisce inoltre un punto di raccordo importante tra i diversi approcci regionali, incluso il RGPD che colloca l'adesione da parte di Paesi terzi alla Convenzione 108 tra i criteri da considerare nella valutazione di adeguatezza di tali Paesi nel contesto dei trasferimenti di dati extra-UE (considerando 105).

Il protocollo contiene diverse novità rispetto all'originaria Convenzione. In particolare: l'ampliamento dei diritti degli interessati, che ora racchiudono anche il diritto a non essere soggetto a decisioni puramente automatizzate e a conoscere la logica del trattamento; nuovi obblighi di trasparenza per i titolari dei dati, nonché quello di adottare un approccio fondato sull'*accountability* e sulla valutazione preventiva dei rischi del trattamento; maggiori garanzie per la sicurezza dei dati, incluso l'obbligo di notificare i *data breach* e di assicurare un approccio di *privacy by design* e *by default*. Il protocollo rafforza inoltre i compiti delle autorità di protezione dati e del Comitato della Convenzione, chiamato a svolgere un ruolo specifico nel processo di valutazione dell'effettivo rispetto dei principi della Convenzione che deve essere assicurato dai Paesi che intendono aderire ad essa, nonché dei Paesi che, pur essendo già parti, saranno comunque sottoposti ad una verifica sulla persistente osservanza della Convenzione.

Proprio alla luce del più ampio ruolo riconosciuto dalla Convenzione modernizzata al suo Comitato, nel corso del 2018 il T-PD ha dunque riaperto la riflessione sui meccanismi di valutazione e *follow up* della Convenzione esaminando le possibili procedure che il futuro Comitato potrà seguire e strutturando il modello di questionario, rivolto alle Parti, che costituirà la base dell'attività di verifica che il Comitato sarà chiamato a svolgere.

Parallelamente al citato lavoro di modernizzazione, crescente è stato l'interesse mostrato da molti Paesi extra-europei nei confronti della Convenzione 108. Il Comitato ha accolto con favore l'avvenuto deposito degli strumenti di ratifica da parte della Repubblica di Capo Verde e del Messico che dal 1° ottobre 2018 sono dunque parti della Convenzione 108 e ha riconosciuto lo status di osservatore all'interno del T-PD al Brasile, all'Autorità di protezione dati del Gabon, oltre che all'associazione *European Digital Rights* (EDRI).

Nel corso dell'anno è inoltre proseguita l'attività del T-PD riguardo all'applicazione dei principi della Convenzione 108 nei diversi settori.

Guida pratica sui trattamenti in ambito di polizia

È stato portato a termine il lavoro sugli aspetti applicativi della raccomandazione (87)15 con l'adozione, a termine di procedura scritta, della guida pratica sull'utilizzo di dati personali in ambito di polizia (15 febbraio 2018, T-PD(2018)01).

Tale documento riconosce l'importanza del trattamento dei dati personali nel contrasto alla criminalità e fornisce orientamenti ed esempi concreti per gli operatori del settore volti ad individuare il corretto equilibrio tra il perseguimento dell'interesse pubblico generale e il rispetto dei diritti delle persone alla vita privata e alla protezione dei dati come previsto dall'art. 8 della Convenzione europea sui diritti umani e dalla Convenzione 108.

La raccolta e l'uso di dati personali per le attività di contrasto costituisce, infatti, un'interferenza con il diritto alla vita privata e alla protezione dei dati. In quanto tale, deve essere basato su adeguate basi normative, perseguire uno scopo legittimo ed essere limitato a ciò che è necessario e proporzionato per raggiungere tale finalità.

La guida pratica fornisce una serie di indicazioni su come rispettare il principio di legalità del trattamento e della raccolta dati, sulle salvaguardie addizionali da applicare al trattamento di dati sensibili, nonché sull'obbligo di trasparenza nei confronti degli interessati e dei loro diritti (quando questo non pregiudichi le indagini o la sicurezza di testimoni). Il documento si sofferma, poi, sull'utilizzo delle nuove tecnologie da parte degli organi di sicurezza di uno Stato, fra cui l'uso dei *Big data* e dell'*Internet of Things (IoT)*, evidenziando le principali pratiche da tenere in dovuta considerazione nello svolgere le attività di indagine e perseguimento dei reati per determinare preventivamente le conseguenze di tali tecnologie sui diritti delle persone, come la valutazione d'impatto preventiva (DPIA) e l'introduzione di meccanismi di *privacy by design*.

Dati relativi alla salute

Sempre con riferimento all'attività relativa all'applicazione settoriale dei principi della Convenzione 108, il Comitato ha portato a termine il processo di revisione della raccomandazione 97(5) approvando un nuovo testo volto ad attualizzare i preesistenti principi di tutela dei dati a fronte delle molte sfide determinate dalla diffusione di nuove tecnologie e della digitalizzazione del settore sanitario (T-PD(2018)06rev). La raccomandazione che (diversamente dall'originaria raccomandazione, riferita ai cd. dati sanitari) muove dalla definizione di "dati relativi alla salute" comprensiva dei dati personali riferibili alla salute mentale o fisica di un individuo (compresi quelli che riguardano la fornitura di servizi di cura o che rivelino informazioni sulla salute passata, presente e futura della persona), è stata adottata dal Comitato dei ministri in data 27 marzo 2019 (raccomandazione (2019)2). Il testo affronta il tema delle basi giuridiche su cui deve fondarsi il trattamento di tali dati, che in base all'art. 6 della Convenzione 108 rientrano nelle categorie "speciali" di dati che necessitano di una tutela rafforzata per il potenziale discriminatorio derivante dal loro utilizzo. Sono previste specifiche garanzie per il trattamento dei dati genetici (particolarmente sensibili per il loro carattere predittivo), nonché sulla condivisione dei dati di salute del paziente da parte di più professionisti del settore al fine di garantire una migliore assistenza medica. Per quanto concerne l'uso di dati ai fini di ricerca scientifica si sottolinea la necessità di rispettare il principio di trasparenza e di assicurare adeguate garanzie (tra cui il consenso dell'interessato). Infine, viene affrontata la questione dei sempre più diffusi dispostivi sanitari mobili (impiantati o meno sulla persona) ai quali si applicano tutti i principi della raccomandazione, in particolare le misure di sicurezza, gli obblighi di trasparenza volti ad informare adeguatamente gli interessati e consentire un controllo effettivo dei propri dati.

ICANN

È proseguito il lavoro sulle linee guida per la protezione dati in ambito ICANN, adottate dal Comitato il 7 settembre 2018 (T-PD(2018)18*final*). Il documento – che specifica che nella nozione di dato personale rientra quella di indirizzo IP – si sofferma sui principi base, riconosciuti a livello internazionale, della protezione dei

dati, anche con riferimento al registro *Whois*, primo tra tutti, la necessità di definire con precisione le legittime finalità dei diversi trattamenti di dati personali posti in essere nel contesto ICANN, astenendosi dai trattamenti per scopi con esse incompatibili e definendo tempi di conservazione dei dati non eccessivi. Particolare attenzione viene prestata alla necessità di individuare le corrette basi giuridiche dei trattamenti, di garantire agli interessati piena trasparenza sul trattamento dei dati che li riguardano, e un agevole esercizio dei propri diritti.

Privacy* e *media

Il Comitato, congiuntamente alla *Steering Committee on Media and Information Society* che nel Consiglio d'Europa si occupa della salvaguardia dei diritti fondamentali (*in primis* della libertà di informazione) nell'ambito dei mezzi di comunicazione e della società dell'informazione, ha approvato le "Linee guida sulla protezione del diritto alla vita privata nei media". Si tratta di un documento ricognitivo, che sintetizza gli standard esistenti del Consiglio d'Europa, e contiene ampi riferimenti alla giurisprudenza della Corte europea dei diritti dell'uomo sul delicato bilanciamento tra diritto alla *privacy* e libertà di manifestazione del pensiero.

Intelligenza artificiale

Particolarmente significativa nel corso dell'anno è stata l'attività del Comitato consultivo sul tema dell'intelligenza artificiale (I.A.). Il lavoro di approfondimento ha portato alla predisposizione di specifiche Linee guida (adottate il 25 gennaio 2019 - T-PD(2019)01). Le Linee guida si rivolgono a *policy makers*, sviluppatori e fornitori di servizi fondati su I.A. e offrono indicazioni affinché l'impiego di tale tecnologia avvenga nel rispetto dei principi della Convenzione 108 modernizzata. Punti cardine delle Linee guida sono la necessità di avere un approccio fondato sulla preventiva valutazione dell'impatto che soluzioni I.A. possono avere su diritti fondamentali e sulla minimizzazione dei relativi rischi per le persone, e l'opportunità di inserire nel processo di valutazione nuove "forme partecipatorie", basate sul coinvolgimento di individui e gruppi potenzialmente colpiti dagli effetti dell'I.A. Ciò per evitare che le scelte sull'utilizzo di tali nuove tecnologie, che rischiano di cambiare radicalmente il nostro modo di stare nella società, siano appannaggio esclusivo di chi detiene il sapere tecnologico.

Nel corso dell'anno il Comitato consultivo ha inoltre adottato un parere sulla compatibilità con la Convenzione 108+ dell'accordo della Conferenza internazionale delle autorità di protezione dati per il trasferimento di dati tra autorità nell'ambito della loro cooperazione (T-PD(2018)13rev), nonché il parere sulla richiesta di accessione alla Convenzione 108 inoltrata dalla Repubblica del Kazakistan nel quale sono state sottolineate le modifiche di cui la normativa kazaka necessiterebbe per assicurare il suo allineamento ai principi della stessa 108.

Premio Stefano Rodotà

Su iniziativa del Comitato, è stato indetto per la prima volta il Premio Stefano Rodotà, in onore e alla memoria del grande giurista, già Presidente del Garante dal 1997 al 2005, rivolto al mondo dell'università e della ricerca per valorizzare e dare visibilità a progetti di ricerca innovativi e originali nel campo della protezione dei dati personali. Il premio è stato assegnato in occasione dell'edizione 2019 della Giornata europea per la protezione dei dati personali.

CAHENF - Comitato *ad hoc* sui diritti dei minori

Si segnala infine che, sempre nell'ambito del Consiglio d'Europa, il 4 luglio 2018 il Comitato dei ministri ha adottato la raccomandazione (2018)7 contenente le Linee guida per rispettare, proteggere i diritti dei minori in ambito digitale, alla cui stesura ha contribuito il Garante nell'ambito del sottogruppo CAHENF-IT del Comitato *ad hoc* sui diritti dei minori.

OCSE - WPSPDE

Il Garante ha proseguito l'attiva partecipazione ai lavori del *Working party on Security and Privacy in Digital Economy* (WPSPDE) dell'OCSE e nel corso della 44ª riunione plenaria (novembre 2018) all'Autorità italiana è stata riconfermata la Vicepresidenza del *bureau* per il 2019. Nel corso dell'anno è stato istituito un

gruppo di esperti incaricato di guidare il futuro lavoro di revisione delle Linee guida OCSE sulla *privacy* (*Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, adottate nel 2013). Come è noto, le prime Linee guida sulla *privacy* di tale organizzazione risalgono al 1980 e rappresentano il primo set di principi di protezione dati internazionalmente riconosciuti. Definiscono i termini rilevanti in materia di protezione dei dati, fornendo otto principi fondamentali per la relativa applicazione nazionale: limitazione della raccolta dati, qualità dei dati, specificazione degli obiettivi, limitazione dell'uso, salvaguardia della sicurezza, apertura, partecipazione individuale e responsabilità (*accountability*). Con la revisione del 2013 è stata riaffermata la validità dei predetti principi che restano la base su cui articolare il nuovo lavoro di aggiornamento. Tuttavia, le *Privacy Guidelines* del 2013 sono state adottate come una raccomandazione contenente un'istruzione del Consiglio OCSE al Comitato per la politica dell'economia digitale (CDEP) di "monitorarne l'attuazione, riesaminare il contenuto e riferire al Consiglio entro cinque anni dalla loro adozione". Pertanto si rende necessaria una nuova revisione che consisterà, innanzitutto, nel monitoraggio delle misure intraprese dai Governi in attuazione delle *Privacy Guidelines* del 2013, così come delle buone pratiche e degli strumenti per affrontare le nuove sfide poste dalla tecnologia nel contesto globale della protezione dati. L'analisi verterà sugli sviluppi della protezione dati in diversi settori: tecnologie, flussi globali di dati, cambiamenti nelle prassi organizzative e nelle pratiche individuali.

Gli enormi cambiamenti nel volume, nella velocità e nella varietà della raccolta ed utilizzo di dati personali (*big data*) e la conseguente trasformazione del ruolo dei dati personali nell'economia e nella società sono stati i principali temi affrontati dagli esperti del WPSPDE: in particolare, si è discusso di come l'ubiquità di *smartphone*, applicazioni e dispositivi IoT ha reso i dati personali accessibili e condivisibili in qualsiasi luogo, portando a flussi di dati su scala globale senza precedenti. In tale scenario, gli esperti delle autorità europee di protezione dati hanno illustrato e portato come esempio l'importante innalzamento degli standard e dei principi di protezione dati che si è verificato con l'adozione del RGPD.

Consultazione sulla protezione dei minori *online*

Il WPSPDE, in vista dell'imminente revisione della raccomandazione sulla protezione dei minori *online*, adottata dal Consiglio OCSE nel 2012, ha, altresì, istituito un gruppo di esperti che guiderà il processo di revisione analizzando i nuovi rischi per i minori *online*. La raccomandazione è stata ritenuta non più al passo con i tempi, essendo trascorsi più di cinque anni dalla sua adozione ed essendo profondamente mutato il contesto delle attività dei minori in rete. Tale analisi sarà fondata sui contributi ricevuti da 34 Paesi membri OCSE che hanno risposto ad un sondaggio del 2017 volto a: raccogliere informazioni sui recenti sviluppi nella politica di protezione dei minori *online*; individuare le aree in cui potrebbe essere necessario aggiornare la raccomandazione OCSE; valutare l'impatto potenziale di ulteriori fattori (nuove tecnologie, utilizzo dati, minacce, ecc.). In tale contesto, si è svolta a Zurigo il 15-16 ottobre la OECD *Expert Consultation sul tema Protecting minors online*. Nel corso dell'incontro sono state presentate esperienze nazionali e ricerche in materia di cyberbullismo e uso di servizi internet da parte di minori discutendo, al contempo, sullo sviluppo di possibili *policy* a carattere transnazionale in grado di arginare l'incidenza di rischi *privacy* e di reati. È stata altresì riaffermata la necessità di un approccio a diversi livelli: l'azione di prevenzione, basata prevalentemente sulla leva dell'istruzione, della consapevolezza, della promozione di una cultura dell'accoglienza e del rispetto della diversità; l'azione tecnologica, basata sulla necessità di individuare e cancellare più rapi-

damente contenuti offensivi, superando le tradizionali limitazioni dello stabilimento territoriale; l'azione del diritto, attraverso un maggiore livello di cooperazione tra differenti paesi e una maggiore interoperabilità tra differenti regimi giuridici. L'Italia ha illustrato il nuovo quadro giuridico introdotto al fine di prevenire e combattere il cyberbullismo introdotto dalla legge nazionale n. 71/2017, che assegna un compito nuovo al Garante, fondato sul meccanismo cd. di *notice* & *take down* (cfr. cap. 9).

Gruppo di Berlino (IWGDPT)

È proseguito il lavoro del "Gruppo di Berlino" (*International Working Group on Data Protection in Telecommunications)* che nel 2018, nelle riunioni di Budapest (9-10 aprile) e Queenstown (29-30 novembre 2018) alle quali il Garante ha partecipato, ha adottato diversi documenti (reperibili sul sito: https://www.datenschutz-berlin.de/datenschutz/zusammenarbeit-und-gremien/#BerlinGroup).

Nella prima riunione il Gruppo ha adottato un documento sull'accesso transfrontaliero ai dati per finalità di *law enforcement* (*Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes*) nel quale si sottolinea che accessi da parte delle autorità giudiziarie e di polizia di uno Stato a dati trattati in altre giurisdizioni non possono prescindere da accordi internazionali tra gli Stati interessati che disciplinino i poteri e i limiti di tali autorità e le modalità di accesso ai dati e devono svolgersi in un quadro di garanzie (la presenza di una richiesta da parte di un'autorità giudiziaria) e di trasparenza (ad es., attraverso rapporti statistici su base annuale delle richieste di accesso pubblicate dagli Stati), offrendo agli interessati, ove possibile (se ciò non compromette la sicurezza nazionale, la vita di persone o l'esito di indagini), la facoltà di esercitare i propri diritti.

Sempre nel corso della riunione di Budapest, il Gruppo ha adottato un documento in materia di veicoli connessi (*connected vehicles*). Il documento offre una panoramica delle diverse applicazioni, degli attuali ed emergenti *stakeholders* presenti nel settore, dei rischi per i diritti delle persone, a cominciare dalla poca trasparenza di trattamenti che possono riguardare non solo il guidatore ma anche i passeggeri e le persone presenti nelle aree che circondano il veicolo, fino ad arrivare ai rischi di uso secondario dei dati in assenza di base giuridica, ad esempio da parte delle assicurazioni. Offre infine una serie di raccomandazioni per garantire il rispetto dei principi di protezione dati nel settore, rivolgendosi ai diversi attori coinvolti, tra cui gli ideatori dei sistemi, i fornitori di servizi e *app,* gli organismi di standardizzazione, gli stessi conducenti, le autorità pubbliche coinvolte e i legislatori. La necessità di limitare il trattamento dei dati a specifiche finalità (guida assistita, sicurezza stradale), di individuare un'idonea base giuridica (in ragione del contesto e della legge applicabile), di rispettare il principio di *privacy by default* (ad es., tramite dispositivi spenti di *default*, che garantiscano una cancellazione immediata dei dati) e, da ultimo, di impiegare soluzioni tecnologiche basate su standard internazionali sono tra le raccomandazioni fornite nel documento.

Nell'incontro di Queenstown il Gruppo ha discusso e adottato il parere in materia di intelligenza artificiale. Anche questo parere mira a evidenziare le sfide principali determinate dallo sviluppo dell'I.A., elenca diversi esempi di applicazione I.A. e fornisce raccomandazioni tecniche affinché i diversi attori coinvolti possano mitigare i rischi che ne derivano per i diritti delle persone, in particolare a sviluppatori e fornitori di servizi, e offre indicazioni sul ruolo delle autorità di protezione dei dati in tale ambito. Dal punto di vista dei contenuti, il parere richiama la necessità di congegnare i sistemi di I.A. nel rispetto dei diritti fondamentali, del diritto alla protezione dati, e del principio di non discriminazione, tenendo conto del loro impatto sugli individui e sulla società in generale. Sottolinea l'urgenza di garantire una vigilanza periodica sull'impatto dei sistemi I.A., una responsabilizzazione dei diversi

attori coinvolti, la trasparenza dei sistemi anche al fine di informare le persone che interagiscano con I.A., nonché l'introduzione di misure di *ethics by design* che sappiano tener conto, fin dal momento della progettazione dei sistemi, dei requisiti necessari ad un utilizzo etico e corretto dell'I.A.

Il Gruppo si è inoltre occupato del tema della localizzazione, ad ampio raggio, per finalità di interesse pubblico, ad esempio attraverso dispositivi installati su veicoli per migliorare traffico, la sicurezza di conducenti o pedoni o per ridurre emissioni inquinanti.

Con il documento di lavoro adottato nella riunione di Queenstown, il Gruppo ha individuato i principali rischi per i diritti delle persone, a cominciare dal controllo sui loro movimenti, nonché la creazione di pregiudizi (*bias*) che finiscono per guidare le scelte della persona sulla base di orientamenti pregressi "fotografati" dai sistemi di localizzazione limitandone la possibilità di libera scelta e ha fornito raccomandazioni, indirizzate ai regolatori, all'industria e alle organizzazione che intendano avvalersi di tali sistemi, affinché il pubblico interesse sia perseguito nel rispetto dei principi di protezione dei dati. Occorre in particolare assicurare la trasparenza (anche attraverso periodici *reminder* agli utenti riguardo persistente localizzazione), una congrua valutazione di impatto prima che i sistemi siano implementati, individuare una adeguata base giuridica privilegiando il consenso per ogni uso ulteriore o per ogni forma di arricchimento dei dati attraverso l'incrocio di fonti diverse, impiegare opzioni di *privacy by design*, ad esempio avvalendosi di pseudonimi temporanei per evitare localizzazioni di lunga durata; assicurare il principio di minimizzazione ad esempio, attraverso l'aggiunta di rumore o la generalizzazione dei dati, nonché l'attuazione di una supervisione attenta da parte delle autorità di protezione su codici di condotta e schemi di certificazione.

Il Gruppo ha altresì avviato una discussione sul trattamento dei dati relativi ai minori (in particolare con riferimento a due temi, i cd. *smart toys* e il *parental control*), nonché sulla tecnologia *blockchain* e i punti di frizione con i principi di protezione dei dati.

***Global privacy enforcement* (GPEN)**

Anche nel corso del 2018 è stato lanciato il *Privacy sweep*, l'iniziativa promossa dal *Global Privacy Enforcement Network* (www.privacyenforcement.net), la rete internazionale nata nel 2010 per rafforzare la cooperazione tra le autorità di protezione dati di diversi Paesi del mondo. Quest'anno l'attività di *Sweep* (indagine a tappeto) ha riguardato il tema del rispetto del principio di responsabilizzazione (*accountability*) e le modalità individuate dai titolari del trattamento per garantire in modo responsabile la conformità alle norme di protezione dei dati. Ogni Autorità partecipante, in tutto da 18 Paesi con 356 organizzazioni intervistate, ha scelto autonomamente lo specifico settore su cui concentrare l'analisi (dal turismo alla salute, dalla pubblica amministrazione alle telecomunicazioni).

In generale, l'indagine internazionale ha mostrato che, nonostante la maggior parte delle organizzazioni (pubbliche e private) analizzate dalle Autorità dimostri una buona comprensione dei concetti base del principio di *accountability*, permangono carenze significative in merito alla concreta attuazione di politiche e programmi specifici a tutela della *privacy*. Pur rilevando esempi di buone prassi, si è osservato, ad esempio, che in molti casi non erano previsti processi specificamente dedicati alla trattazione di reclami o alle richieste degli interessati, né meccanismi idonei a gestire adeguatamente eventuali violazioni alla sicurezza dei dati.

Sul fronte interno, il Garante ha analizzato le regioni e le province autonome nonché le loro principali aziende partecipate (cd. *in house*) – che effettuano rilevanti trattamenti di dati personali per lo svolgimento di compiti di interesse pub-

blico. L'indagine svolta in Italia ha visto un alto tasso di risposta (circa 70 questionari ricevuti), ma lo stato di adeguamento ai principali adempimenti ha fatto emergere un quadro ancora non soddisfacente. Anzitutto, per quanto concerne la *governance* della *privacy*, un quinto delle regioni non ha ancora adottato una procedura interna per la gestione dei dati personali o non l'ha applicata correttamente nelle attività interne. Quasi tutte, però, hanno incaricato una figura competente in materia di *governance* e gestione della protezione dati a un livello gerarchico sufficientemente elevato. Sul fronte della formazione, della consapevolezza e del suo monitoraggio, la maggior parte delle regioni e delle società *in house* riconoscono l'importanza di un'adeguata formazione dei dipendenti in materia di *privacy*, ma non sempre hanno posto in essere un costante monitoraggio di quest'ultima. Per quanto riguarda la trasparenza nel trattamento dei dati, essa è garantita attraverso specifiche informative agli interessati che, di solito, sono aggiornate e facilmente accessibili, sebbene alcune organizzazioni appaiono limitarsi a presentare la sola *privacy policy* del sito web. Altro dato preoccupante è emerso nella gestione degli incidenti di sicurezza (*data breach*) in cui il 24% delle società e il 48% delle Regioni non hanno definito *policy* e procedure per la gestione dei rischi, incluso tra l'altro, la notifica all'Autorità e, in caso di alto rischio per le libertà e i diritti degli interessati, anche la comunicazione a questi ultimi. Un quarto delle organizzazioni sembra inoltre non disporre di un registro per documentare le violazioni subite. Da ultimo, è emerso che il 24% delle società *in house*, ma addirittura il 58% delle regioni, non hanno processi documentati per la valutazione dei rischi sulla protezione dei dati personali (DPIA), in relazione all'utilizzo di nuovi prodotti, tecnologie o servizi. La maggior parte dei soggetti analizzati ha comunque creato un registro dei trattamenti effettuati.

22.4. *Le conferenze internazionali ed europee*

40ª ICCDPC

La Conferenza internazionale delle autorità di protezione dati, organizzata dal Garante europeo per la protezione dati congiuntamente all'autorità bulgara e dal titolo "*Debating Ethics: Respect and Dignity in Data Driven Life*" si è tenuta a Bruxelles dal 22-26 ottobre. Come di consueto la conferenza si è articolata nella sessione aperta – nel corso della quale si è discusso dei molti cambiamenti dettati dalla digitalizzazione e della necessità di garantire, oltre all'osservanza dei principi di protezione dei dati dettati dalla legge, anche una visione "etica" dei cambiamenti tecnologici in corso per garantire una piena autonomia delle persone, evitare forme di manipolazione, sorveglianza massiva e autocensura – e nella sessione chiusa, in cui le autorità hanno adottato una dichiarazione e cinque risoluzioni (reperibili sul sito web: https://icdppc.org).

Nella dichiarazione su etica e protezione dei dati nell'intelligenza artificiale, che ha visto tra gli estensori anche il Garante, vengono definiti sei principi cardine a tutela dei diritti fondamentali e della dignità della persona che dovrebbero essere rispettati, a livello globale, da ogni soggetto coinvolto nello sviluppo o nell'utilizzo di sistemi di intelligenza artificiale (I.A.). In base ai principi delineati dalle autorità di protezione dati, la progettazione e l'utilizzazione delle tecnologie di I.A. dovrebbero essere conformi, ad esempio, al principio di correttezza, garantendo che vengano utilizzate soltanto per facilitare lo sviluppo umano senza ostacolarlo o minarlo. Nel documento si sottolinea l'importanza di responsabilizzare tutti i soggetti coinvolti, attivando forme di vigilanza continua e definendo processi verificabili di *governance* dell'I.A., nonché la necessità di migliorare la trasparenza e l'intelligibilità

di tali sistemi, fornendo informazioni adeguate sulle loro finalità e sugli effetti causati, allo scopo di verificarne il costante allineamento con le aspettative delle persone e permettere un effettivo "controllo umano". Particolare attenzione dovrà essere posta alla "progettazione responsabile" applicando, sin dalle sue prime fasi, i principi di *privacy by design* e *by default*.

In considerazione delle sfide poste dallo sviluppo dell'intelligenza artificiale, le autorità hanno poi deciso di istituire un gruppo di lavoro permanente che possa monitorarne gli sviluppi. Il testo della dichiarazione è stato sottoposto a consultazione pubblica, al fine di ampliarne la portata e favorirne la condivisione degli obiettivi.

Durante i lavori, le autorità hanno inoltre approvato cinque risoluzioni. Quella dedicata all'*e-learning*, pur enfatizzando i benefici nell'utilizzo di strumenti *online* dedicati alla formazione di giovani ed educatori, invita al rispetto della *privacy* degli utenti sin dalle prime fasi di progettazione di tali piattaforme. Una seconda risoluzione è rivolta al miglioramento della cooperazione tra autorità di protezione dei dati e quelle dei consumatori, al fine di rendere gli strumenti di tutela internazionale più efficaci. Altre tre risoluzioni adottate riguardano il futuro della Conferenza internazionale, regole e procedure per migliorarne il lavoro, nuovi parametri e strumenti per il monitoraggio e la comparazione del livello di protezione della *privacy* su scala internazionale.

***Spring conference* 2018**

Il 3-4 maggio 2018 si è tenuta a Tirana la 28ª *Spring conference* delle autorità europee di protezione dati, alla quale ha partecipato una delegazione del Garante presieduta dal Segretario generale, che ha preso parte alla sessione sul ruolo delle autorità di protezione dati nell'ambito della cooperazione con i servizi di *intelligence*. La Conferenza è stata anche l'occasione per fare il punto sul processo di modernizzazione della Convenzione 108/1981 del Consiglio d'Europa, per discutere della protezione dei dati personali nell'ambito di polizia e giustizia, anche in relazione all'impiego di sistemi di giustizia predittiva, dell'influenza degli standard europei su altri sistemi giuridici, della protezione dei dati in ambito umanitario, e dell'analisi dei dati e la profilazione a fini politici, in particolare con riferimento al caso Cambridge Analytica. Si è inoltre dibattuto del futuro della Conferenza alla luce del documento di discussione predisposto dal relativo gruppo di lavoro, nonché del tema della *membership* di Paesi extra-europei (ovvero le Parti della Convenzione 108 che non appartengono al Consiglio d'Europa): al riguardo la Conferenza ha concluso per l'opportunità di mantenere il carattere europeo della *Spring conference*, anche per evitarne la sovrapposizione con altri *fora* analoghi di carattere internazionale, riservandola cioè ai Paesi appartenenti al Consiglio d'Europa, così come previsto dalle regole procedurali adottate nella precedente conferenza di Limassol del 2017.

9ª Conferenza internazionale - Mosca

L'Ufficio ha inoltre preso parte alla 9ª Conferenza internazionale "*Personal Data Protection*" (Mosca, 8 novembre 2018) organizzata dall'Autorità russa per la supervisione delle comunicazioni, delle tecnologie, dell'informazione e delle comunicazioni di massa. Le tematiche in discussione hanno riguardato in particolare l'adeguamento della protezione dei dati personali alla progressiva digitalizzazione dei flussi dati nell'ambito dello sviluppo della società dell'informazione; le principali tendenze nello sviluppo di nuove regole per la protezione dei dati, con particolare riferimento al RGPD e alla Convenzione 108 modernizzata; *big data* con riguardo alle norme applicabili, tecnologie, metodologie di implementazione e modelli di regolazione; le caratteristiche tecnologiche della rete internet in particolare con riferimento ai servizi globali e problemi legati al controllo dei dati a livello nazionale e individuale (*data sovereignity*). Il Garante nella sessione "*International Expert*

Meeting" ha presentato una relazione dal titolo "*Value and Impact of the Accountability principle under GDPR*".

22.5. *I progetti per l'applicazione del RGPD finanziati dall'UE: T4DATA e SMEDATA*

T4DATA

Il Garante ha proseguito le attività previste dal progetto europeo T4DATA, avviato nel 2017 nell'ambito della selezione della Commissione europea denominata *Support training activities on the data protection reform*, e coordinato dalla Fondazione Basso in consorzio con il Garante, nonché le Autorità di protezione dati di Spagna, Polonia, Croazia e Bulgaria.

Il progetto, che si rivolge ai soggetti pubblici, si concentra sulla formazione relativa ai nuovi adempimenti previsti dal Regolamento e si articola in due fasi, la prima dedicata alle autorità di protezione di dati, finalizzata all'affinamento delle nozioni e delle implicazioni pratiche del Regolamento, e la seconda, nella quale le stesse autorità agiranno come formatori degli enti pubblici sugli adempimenti dettati dal RGPD e in particolare dei loro Rpd, figure obbligatorie nel settore pubblico ai sensi dell'art. 37, comma 1, lett. *a*).

Il Garante ha partecipato, insieme ai *partner* del progetto, a tre eventi principali: il 13 marzo 2018 si è tenuta a Zagabria la prima riunione finalizzata all'organizzazione delle attività di formazione. Il Garante ha poi ospitato il primo seminario interno (11-13 giugno) volto ad approfondire le diverse novità del RGPD, proprio nell'ottica degli adempimenti cui i Rpd sono tenuti. Le autorità consorziate si sono inoltre riunite a Varsavia (8-10 ottobre) per scambiare informazioni sulle diverse esperienze nazionali, in particolare *best practices* e attività divulgative, fino a quel momento maturate con riferimento al RGPD ormai interamente applicabile.

A dicembre è stato ultimato il Manuale operativo sul Rpd preparato dagli esperti del progetto, insieme ai *partner,* che servirà da base di partenza per i contenuti dei *webinar* formativi da svolgersi nel corso del 2019 insieme a quattro ulteriori seminari locali (che si terranno in differenti regioni italiane all'interno della fase di divulgazione del progetto in collaborazione con altre istituzioni pubbliche locali, regionali e nazionali).

SMEDATA

A fine 2018 è stato avviato un altro progetto, anch'esso finanziato dalla Commissione europea europeo, denominato SMEDATA (www.smedata.eu), in partenariato con alcuni enti bulgari – fra cui l'Autorità di protezione dati, capofila del progetto, e alcune associazioni professionali di avvocati e giuristi – nonché l'Università Roma Tre che affiancherà il Garante nello sviluppo della programmazione in Italia. Il progetto è volto a fornire alcuni strumenti pratici e interpretativi per supportare e formare i rappresentanti e gli esperti legali delle piccole e medie imprese (*Small and Medium Enterprises* – SMEs), sia italiane che bulgare, nell'applicazione e negli adempimenti del RGPD. La durata del progetto è biennale (dicembre 2018 - dicembre 2020) e coinvolgerà il Garante nella prima fase di predisposizione del sito, dei materiali divulgativi e, successivamente, nell'organizzazione di seminari locali rivolti agli esperti legali delle PMI italiane, nella diffusione di un'applicazione web di supporto agli adempimenti del Regolamento e nella conferenza finale che si terrà a Roma.

23 Attività di normazione tecnica internazionale e nazionale

Il Garante ha proseguito la collaborazione in tema di elaborazione di norme tecniche internazionali nell'ambito del *Working Group 5* del sottocomitato SC27, che si occupa della sicurezza delle informazioni all'interno del comitato tecnico JTC1 dell'organizzazione internazionale per la normazione (ISO). Il gruppo di lavoro segue gli aspetti di sicurezza nella gestione delle identità relativamente alle tecnologie biometriche e alla protezione dei dati personali. Armonizzando la propria posizione con quelle delle altre autorità di protezione dati tramite il WP29, che ha una *liason* in proposito con ISO, l'Autorità ha seguito lo sviluppo delle norme tecniche di seguito riportate:

– ISO 20889 - *Privacy enhancing data de-identification techniques*: standard che fornisce una descrizione delle tecniche di de-identificazione utili nella progettazione di misure atte a rafforzare la *privacy* in accordo con i princìpi previsti dalla norma ISO/IEC 29100 *privacy framework*;

– ISO 29184 - *Guidelines for online privacy notice and consent*, che definisce una serie di requisiti per fornire l'informativa e acquisire il consenso *online* in modalità *user friendly*;

– ISO 27552 - *Information technology - Security techniques – Enhancement to ISO/IEC 27001 for privacy management – Requirements*, che stabilisce i requisiti di un sistema di gestione della *privacy* delle informazioni (PIMS) a completamento di un sistema di gestione per la sicurezza delle informazioni (ISMS - ISO 27001);

– ISO 27570 - *Privacy guidelines for smart cities*, che fornisce linee guida sull'utilizzo degli standard *privacy* nell'ambito *smart cities*;

– ISO 27555 - *Establishing a PII deletion concept in organizations*, che fornisce linee guida per la cancellazione dei dati personali che includono la classificazione dei dati, la definizione di tempi di cancellazione/periodi di mantenimento, di classi di cancellazione, di requisiti di implementazione nonché processi e responsabilità.

Collaborazione è stata assicurata nell'ambito del *Project Committee* (PC) 317 di ISO, istituito dal *Technical Management Board* a febbraio 2018, per lo sviluppo di una norma tecnica internazionale su "*Consumer protection: Privacy by design for consumer goods and services*".

L'Autorità ha inoltre contribuito all'elaborazione di norme tecniche europee nell'ambito del comitato tecnico 8 del CEN CENELEC che si occupa dello sviluppo di norme tecniche riguardanti *Privacy management in products and services* su mandato della Commissione europea (Direzione generale sicurezza e affari interni) per l'elaborazione di norme tecniche per la *Privacy by design*.

Del pari è proseguita la collaborazione con Unifo, l'ente di normazione federato con Uni (Ente nazionale italiano di unificazione), contribuendo all'elaborazione della circolare tecnica n° 03/2018 Accredia "Disposizioni in materia di certificazione e accreditamento per la conformità alla norma Uni 11697:2017 - Profili professionali relativi al trattamento e alla protezione dei dati personali".

24 L'attività di comunicazione, informazione e di rapporto con il pubblico

24.1. *La comunicazione del Garante: profili generali*

L'attività di informazione e comunicazione dell'Autorità è stata realizzata attraverso una serie di interventi centrati soprattutto sulle rilevanti novità introdotte dal RGPD e sulle grandi questioni legate alla tutela dei diritti fondamentali delle persone nel mondo digitale: le implicazioni etiche della tecnologia; le grandi piattaforme; i *big data*, gli algoritmi ad uso sociale; la pervasività delle diverse forme di controllo e la raccolta dei dati; la profilazione, anche a fini di condizionamento dell'opinione pubblica; la *cybersecurity*. L'anno appena trascorso è stato caratterizzato da numerosi clamorosi fatti che hanno messo a rischio la sicurezza informatica di milioni di persone in tutto il mondo. E sotto il profilo degli utilizzi illeciti dei dati personali sulle piattaforme *social*, va ricordato il caso Cambridge Analytica, che ha visto l'intervento da parte del Garante, volto ad accertare le violazioni dei dati personali degli utenti italiani e a mettere in guardia sui rischi per la libertà delle persone da forme distorte di influenza politica.

A settembre ha preso il via il cd. *privacy sweep* 2018, l'indagine internazionale "a tappeto" dedicata, quest'anno, al principio di responsabilizzazione (*accountability*) del titolare del trattamento dei dati, introdotto dal RGPD in tutta Europa. Sotto osservazione le misure che titolari o responsabili del trattamento hanno scelto per garantire e dimostrare il rispetto delle norme in materia di protezione dei dati.

L'iniziativa viene gestita dal GPEN – *Global Privacy Enforcement Network* – la rete internazionale creata per consolidare la cooperazione tra le Autorità della *privacy* dei diversi Paesi nel mondo conta, ad oggi, più di 60 autorità garanti.

Il Garante italiano quest'anno, ha indirizzato la sua attenzione verso le regioni, le province autonome e le loro società controllate, che svolgono trattamenti di dati personali per l'adempimento di compiti di pubblico interesse. Oltre a quella italiana, altre 17 autorità garanti della *privacy* di altrettanti Paesi del mondo hanno partecipato all'indagine.

Altri ambiti nei quali l'Autorità è intervenuta con finalità informativa sono stati: il censimento permanente; l'uso illecito dei dati personali dei lavoratori; la pubblicazione di informazioni sulle vittime di violenza sessuale; il trattamento di dati dei clienti da parte di Uber; l'*hate speech*; il diritto all'oblio; la sicurezza dei grandi *database* pubblici e privati; le misure antiriciclaggio; gli *smart toys*; le nuove disposizioni riguardanti la carta di identità elettronica per i minori. In via generale e per sintetizzare, le attività di comunicazione e informazione, nell'anno 2018, sono state finalizzate alla diffusione di quella "cultura della *privacy*" necessaria per promuovere sviluppo economico e libertà, efficienza amministrativa e dignità della persona.

Altre questioni alle quali, considerato il loro particolare impatto economico e sociale ed i propri interventi in materia, l'Autorità ha dato ampio rilievo nella sua attività di informazione, sono state la fatturazione elettronica (cfr. par. 4.5.2) e il telemarketing aggressivo (cfr. par. 10.2).

Il 2018 può essere considerato un anno spartiacque per la *data protection*, con la piena applicazione del RGPD, comportando una serie di innovazioni normative e

procedurali che sono state il principale oggetto dell'attività comunicativa e informativa curato e sviluppato dall'Autorità.

Le novità introdotte sono state inoltre oggetto di un ciclo di eventi promossi dal Garante per supportare i soggetti pubblici e privati a dare attuazione al RGPD, tra i quali si menziona l'incontro con gli atenei e gli enti di ricerca italiani, svoltosi a Roma, in aprile, con il fine di incentivare la collaborazione del sistema dell'istruzione affinché si creino le condizioni per stimolare nei giovani la consapevolezza sul tema della condivisione dei dati personali.

Con l'obiettivo di favorire la formazione delle autorità nazionali di controllo e dei Responsabili per la protezione dei dati negli organismi pubblici nell'applicazione del RGPD, è stato lanciato un progetto formativo transnazionale T4DATA, che ha visto il primo incontro nel mese di giugno e un secondo ciclo di formazione a Varsavia, in ottobre, durante il quale sono stati messi a punto la realizzazione di appositi *webinar* per la formazione *online* degli operatori del settore.

Su tutte le questioni sulle quali il Garante è intervenuto i *media* hanno mantenuto sempre una costante attenzione. Il Servizio relazioni esterne e media ha selezionato circa 58.140 articoli nazionali di interesse per l'Autorità e 1.904 articoli provenienti dalla rassegna estera. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali, delle testate *online* e *blog* che hanno trattato i temi legati alla *privacy* sono state 9.300, quelle relative all'attività del Garante 5.690. Gli articoli aventi per oggetto le interviste, interventi e dichiarazioni del Garante sono stati 556 su stampa e web, mentre 102 su radio e tv.

Si contano, infine, 553 articoli relativi ai comunicati stampa e 468 relativi agli argomenti delle *newsletter*.

24.2. *I prodotti informativi*

Nel corso del 2018 sono stati diffusi 38 comunicati stampa e 12 *newsletter*. Le puntate della rubrica radiofonica *Bollettino del Garante* sono state 18.

La *newsletter* del Garante è una pubblicazione periodica, giunta al XX anno di diffusione (per un totale di 448 numeri e di 1.534 notizie). Nata in forma cartacea, oggi è diffusa esclusivamente in formato elettronico a redazioni, professionisti, amministrazioni pubbliche, imprese e singoli cittadini che ne fanno esplicita richiesta o si iscrivono *online*. Al 31 dicembre la lista di distribuzione contava oltre 20.527 destinatari effettivi. In un'ottica *mobile responsive* ne sono state riviste la struttura e la grafica e sviluppata una nuova impaginazione che ne valorizza la presenza di immagini e foto. La *newsletter* è un valido strumento, che consente un ampio approfondimento rispetto ai più importanti provvedimenti adottati dall'Autorità in vari settori, alla sua attività in ambito nazionale, europeo ed internazionale, alle molteplici iniziative legate alla protezione dei dati personali e alla tutela dei diritti fondamentali, fornendo un vasto panorama di questioni e problematiche. Tra i numerosi provvedimenti adottati dal Garante viene operata una scelta tra quelli di maggiore interesse pubblico che vengono rielaborati in chiave giornalistica. Sul sito è sempre possibile consultare l'archivio tematico della pubblicazione che raccoglie, divise per categorie, i 20 anni di articoli prodotti dalla redazione. *Online* è consultabile anche l'intero archivio dei comunicati stampa.

Nell'attività di divulgazione va ricordata la rubrica "*Il Bollettino del Garante della* Privacy", in onda su Radio Radicale: un contributo informativo, tenuto dal Responsabile delle comunicazioni esterne dell'Autorità, che illustra i principali

provvedimenti adottati dal Garante e, più in generale, le tematiche legate alla protezione dei dati personali. Nel 2018 i temi trattati hanno riguardato tra l'altro l'anonimato delle vittime di violenza sessuale; l'uso delle foto tratte da internet; il nuovo *software* per le ricerche nell'archivio Afiss da parte delle Forze di polizia; la tutela dei dati dei donatori a favore degli enti *no-profit*; la geolocalizzazione dei lavoratori di servizi di vigilanza privata e trasporto valori; la raccolta delle impronte digitali nella pa; i dati degli invalidi *online*.

24.3. *I prodotti editoriali e multimediali*

La tipologia dei prodotti editoriali del Garante – opuscoli, video, infografiche, schede – si fonda su una strategia integrata di comunicazione che utilizza le potenzialità della rete ed in maggior misura i *social* per nuove modalità di divulgazione.

I numerosi prodotti multimediali realizzati hanno offerto un ventaglio ampio di risposte alle molteplici esigenze conoscitive da parte dei cittadini e semplificato la comprensione dei principali provvedimenti adottati dall'Autorità e delle nuove norme europee che interessano i diversi aspetti della protezione dei dati personali.

Anche avvalendosi del supporto di consulenti grafici ed informatici esterni, il Servizio relazioni esterne e media – con l'intento di migliorarne la funzionalità – ha ridefinito ed aggiornato la struttura informativa, i contenuti e la grafica della *home page* del sito istituzionale dell'Autorità. Il *restyling* ha ottimizzato l'*appeal* estetico, facilitato l'accesso ai documenti e migliorato la lettura da dispositivi mobili. L'adattamento al *mobile responsive* di oltre 100 schede e pagine informative – in larga parte concentrate nelle sezioni dedicate al RGPD, al Codice ed alla trasparenza – ha richiesto uno sforzo notevole in termini di progettazione, sviluppo e manutenzione.

Tutta la sezione appositamente dedicata al RGPD, con informazioni e documenti di interesse, è stata totalmente riorganizzata ed aggiornata, ma anche ampliata con l'aggiunta di tre nuove schede infografiche: Regolamento (UE) 2016/679: una sintesi per enti ed aziende (doc. web n. 9002768); Conosci i principali diritti previsti dal Regolamento (EU) (doc. web n. 9057278); Regolamento (UE) il bilancio dei primi 4 mesi di applicazione (doc. web n. 9045132); ed una pagina informativa sulla violazione dei dati personali (*data breach*) (www.garanteprivacy.it/regolamentoue/databreach).

Le schede infografiche e le pagine informative si sono confermate, anche nel 2018, il canale comunicativo principale per veicolare informazioni e concetti normativi in maniera più sintetica, ma sempre rigorosa. Tali prodotti sono particolarmente adatti alle esigenze di diffusione attraverso il web e i *social media*.

Del testo del RGPD il Garante ha elaborato una versione digitale arricchita con riferimenti ai considerando, aggiornata alle rettifiche pubblicate sulla GUUE 23 maggio 2018, n. 127. Il testo è scaricabile in formato pdf dal sito del Garante (doc. web n. 6264597); anche il testo coordinato del Codice con le modifiche introdotte dal decreto legislativo n. 101/2018 è disponibile *online* (doc. web n. 9042678).

A marzo è stata pubblicata la nuova versione aggiornata della "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali" (realizzata in collaborazione con il Servizio relazioni comunitarie ed internazionali). La Guida traccia un quadro generale delle principali innovazioni introdotte dalla normativa e fornisce indicazioni utili sulle prassi da seguire e gli adempimenti da attuare per dare corretta applicazione alla normativa. La versione *online* dell'opuscolo, in formato ipertestuale è disponibile sul sito dell'Autorità (doc. web n. 6807118).

Fa parte della campagna di comunicazione che l'Autorità ha attivato con la sezione appositamente dedicata all'informazione sul RGPD, anche il *video spot* intitolato "La protezione dei dati è un diritto di libertà" (doc. web n. 8581971) che – tra aprile e maggio – è stato trasmesso sulle reti radio e tv della Rai, utilizzando gli spazi televisivi destinati alla comunicazione di utilità sociale. L'Ufficio ne ha progettato il *concept* e realizzato l'adattamento tecnico e contenutistico, in coordinamento con il Dipartimento editoria della Presidenza del Consiglio dei ministri.

Nel quadro di un più vasto progetto dedicato all'informazione nel campo dell'internet delle cose (in riferimento alle tematiche della *data protection*) è stata ideata e realizzata una campagna informativa dedicata agli *smart toys* (giocattoli intelligenti). La campagna comprende una pagina tematica aggiornata alla luce delle novità tecnologiche e giuridiche (vwww.garanteprivacy.it/iot/smarttoys).

Per quanto riguarda il settore editoriale, nella Collana del Garante, "Contributi", dedicata a testi di approfondimento sulle problematiche riguardanti la protezione dati e la tutela della dignità della persona, si è aggiunto il volume "Uomini e macchine. Protezione dati per un'etica del digitale" che raccoglie i contributi degli studiosi ed esperti intervenuti al convegno organizzato dall'Autorità in occasione della giornata europea 2018. Il volume è disponibile in formato elettronico (doc. web n. 7415998).

24.4. *Le manifestazioni e le conferenze*

Il 17 gennaio il Presidente è intervento al Convegno "Sorveglianza da parte dei Servizi di *intelligence*: Garanzie dei diritti fondamentali e mezzi di ricorso nell'Ue – Volume II: prospettive e aggiornamento normativo". L'evento, che si è tenuto a Roma presso Palazzo Giustiniani, è stato organizzato dall'Agenzia dell'Unione europea per i diritti fondamentali e dal Comitato parlamentare per la sicurezza della Repubblica. Il presidente Soro, nel corso del suo intervento, ha trattato il tema del rapporto tra libertà e sicurezza e ha affermato che la vera sfida consiste nel rendere la tecnologia una risorsa tanto per la sicurezza quanto per la libertà. Il modo migliore per difendere la nostra sicurezza è proteggere i nostri dati, solo così il rapporto tra libertà e sicurezza non sarà declinato nei termini di un gioco a somma zero e tanto la tecnologia quanto il diritto potranno dirsi davvero al servizio dell'uomo.

In occasione della Giornata europea della protezione dei dati personali del 2018, l'Autorità ha organizzato il convegno dal titolo "Uomini e Macchine. Protezione dei dati per un'etica del digitale", svoltosi a Roma, il 30 gennaio nell'Aula del Palazzo dei gruppi parlamentari. La giornata, promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte le Autorità europee per la *privacy*, viene celebrata in tutta Europa a partire dal 2007 e ha come obiettivo quello di sensibilizzare i cittadini sui diritti legati alla tutela della vita privata e delle libertà fondamentali (doc. web n. 7415998). Il convegno organizzato dal Garante è stato una preziosa opportunità di discussione e confronto su un tema di particolare rilevanza per la nostra società presente e futura, come quello del rapporto tra "uomini e macchine", nell'intento di tracciare un orizzonte etico della tecnologia, esplorando le frontiere più avanzate: dalle tecnologie indossabili agli oggetti "intelligenti", dal "corpo elettronico" all'algoritmo come strumento di controllo sociale, dalla pervasività delle diverse forme di controllo e raccolta dei dati ai rischi per la libertà dell'uomo derivanti da una progressiva delega alla tecnologia di scelte e responsabilità.

Al convegno, articolato in tre sessioni moderate dalle componenti dell'Autorità Augusta Iannini, Licia Califano, Giovanna Bianchi Clerici, hanno partecipato Vito

Mancuso, Antonio Punzi, Luisa Crisigiovanni, Massimo Sideri, Edoardo Fleischner, Francesco Grillo. I lavori, aperti dal presidente Antonello Soro, sono stati chiusi dalla sottosegretaria alla Presidenza del Consiglio dei ministri, Maria Elena Boschi.

Il presidente Soro, nel suo discorso di apertura dei lavori ha sostenuto che "Con internet, la tecnologia da strumento si è fatta dimensione, ecosistema in cui siamo così profondamente immersi da non renderci conto, fino in fondo, delle sue implicazioni". Di qui l'importanza delle norme del RGPD sulla trasparenza del processo decisionale automatizzato, dei suoi criteri e delle sue conseguenze, esigendo la possibilità di un intervento umano, contrastando la delega assoluta al cieco e neppure neutro determinismo dell'algoritmo. E se, come ha concluso Soro, il diritto in generale svolge oggi, sempre più, una funzione di umanizzazione della tecnica, "il diritto alla protezione dei dati rappresenta una straordinaria risorsa per mantenere la persona, nella sua libertà e nella sua responsabilità, al centro della società digitale". Nella prima sessione: "Intelligenze delle macchine e libertà dell'uomo", coordinata da Augusta Iannini, vicepresidente dell'Autorità, sono intervenuti il teologo Vito Mancuso e Antonio Punzi, ordinario di metodologia della scienza giuridica. Nella seconda sessione "Giocattoli intelligenti e oggetti che ci sorvegliano", sono intervenuti Luisa Crisigiovanni, membro dell'esecutivo BEUC e Massimo Sideri, direttore del Corriere Innovazione. A coordinare il dibattito Licia Califano, componente del Garante. Nella terza sessione, coordinata da Giovanna Bianca Clerici, componente del Garante, è stato approfondito il tema "Corpo elettronico e tecnologie indossabili" con le relazioni di Edoardo Fleischner, docente di comunicazione crossmediale e Francesco Grillo docente di economia politica, con conclusione dei lavori della sottosegretaria di Stato, Maria Elena Boschi.

Nella *lectio magistralis* dal titolo: "*Big data*, intelligenza artificiale e protezione dei dati", tenuta il 22 marzo alla Lumsa, il presidente Soro ha affrontato le molteplici possibilità innovative, offerte dai *big data*, di sviluppare modelli interpretativi, analitici e predittivi di fenomeni e comportamenti umani, impensabili solo fino a pochi anni fa, che hanno conferito ai dati un valore inestimabile. Il possesso e l'utilizzo dei *big data* sta segnando profondamente il destino della democrazia, dell'organizzazione sociale e della prosperità economica mondiale: ciò che segnerà le sorti della democrazia sarà probabilmente, non solo il possesso dei dati, ma la loro gestione nel rispetto dei diritti e delle libertà. Deve essere ostacolata l'idea per cui la persona è considerata una "miniera a cielo aperto" e i suoi dati "petrolio" da cui attingere per elaborare profili personali, sociali, di gruppo. Il rischio di consegnare a poche aziende digitali il potere di conoscere fatti utili a governare ed influenzare le nostre scelte è molto alto ed accentua la distanza tra valorizzazione economica ed utilità sociale, con una serie di pericoli che vanno dalla discriminazione sociale fondata sulla scelta algoritmica alla marginalizzazione della persona nei processi decisionali. Sono, questi, alcuni dei concetti espressi dal presidente Soro.

L'attività di divulgazione e approfondimento, compiuta attraverso la partecipazione del Presidente e delle componenti del Collegio nonché del Segretario generale e dei dirigenti a seminari, incontri, convegni ed altre iniziative aventi ad oggetto il nuovo RGPD è stata intensa e costante. Il Garante ha svolto una diffusa azione di divulgazione pubblica, volta ad illustrare le nuove disposizioni e a chiarire le procedure operative da seguire. Numerosi gli aspetti trattati dai componenti del Collegio e dai dirigenti dell'Autorità nel corso degli eventi cui hanno preso parte: la nuova figura del responsabile della protezione dei dati personali (Rpo); la valutazione d'impatto o Dpia; il registro delle attività di trattamento; il principio di responsabilizzazione (*accountability*); il diritto alla portabilità dei dati e il diritto all'oblio; *privacy by design* e *by default*; le novità sul trattamento dei dati previdenziali e sanitari.

Tra i tanti va ricordato il seminario formativo dal titolo "Il nuovo Regolamento UE in materia di protezione dei dati personali. Il Garante incontra l'Amministrazione economico finanziaria", svoltosi il 27 marzo a Roma. Nel corso dell'incontro – organizzato da Sogei, *partner* tecnologico del Mef in collaborazione con il Garante – è emerso come la raccolta e l'analisi dei dati personali sia una componente strategica nell'evoluzione dell'economia digitale e quanto sia necessario che la p.a. garantisca sempre il rispetto dei parametri di riservatezza, integrità e trasparenza dei dati. Nel suo intervento il presidente Soro ha sottolineato come "il Regolamento UE rappresenti una straordinaria occasione per l'innovazione e lo sviluppo delle imprese e delle amministrazioni, che potranno così cogliere le numerose opportunità offerte dalle nuove tecnologie, rafforzando al contempo, le garanzie per la protezione dei dati personali dei cittadini".

Il segretario generale Busia, il 9 maggio, ha preso parte alla tavola rotonda "*Accountability* & consapevolezza", organizzata a Roma su iniziativa dell'Istituto superiore di studi sanitari "Giuseppe Cannarella" e dall'"Osservatorio 679". In tale occasione si sono incontrati i maggiori esperti del settore per riflettere sugli aspetti più innovativi e decisivi dal punto di vista strutturale e legislativo del principio di *accountability*, espresso nel RGPD, che rappresenta la novità più rilevante. Il segretario Busia ha illustrato i nuovi diritti dell'interessato ed ha affrontato in particolare quello alla portabilità dei dati introdotto dal RGPD.

Il 24 maggio a Bologna, alla vigilia dell'entrata in vigore del RGPD, si è svolto l'evento dal titolo: "Il Garante incontra i Responsabili della protezione dei dati (Rpd). Prime indicazioni per l'attuazione dei compiti e per la definizione delle modalità di relazione con l'Autorità", organizzato in collaborazione con la Regione Emilia Romagna. L'appuntamento, che ha visto la partecipazione dei Responsabili della protezione dei dati pubblici e privati, rientra in un ampio progetto promosso dall'Autorità finalizzato a favorire la conoscenza delle nuove norme e offrire un supporto nell'attuazione degli adempimenti previsti da RGPD.

Il presidente Soro, nel suo intervento, ha sottolineato come il RGPD sposti il cardine della normativa dalla tutela dell'interessato alla responsabilità del titolare e dei responsabili del trattamento. Il responsabile della protezione dei dati è una figura su cui si gioca la scommessa della sicurezza, un elemento di vantaggio competitivo.

E ancora, il 16 ottobre il Garante è intervenuto anche all'inaugurazione del ciclo dei seminari per *Data protection officer* (Dpo) presso l'Università degli studi di Salerno, e al VIII Convegno annuale promosso da Diritto delle nuove tecnologie e studi giuridici per l'innovazione dal titolo "Protezione dei dati personali tra Regolamento Ue e nuovo Codice *privacy*: un primo bilancio applicativo", presso l'Università Bicocca di Milano.

Il 14 novembre, il Dipartimento di giurisprudenza della Luiss ha organizzato l'incontro dal titolo "La rivoluzione mancata. A proposito di riforma della disciplina delle intercettazioni", al quale ha preso parte il presidente Soro. "L'aver reso pubblico il processo, e non arbitrario – ha detto Soro in apertura del suo intervento – è stata certamente una conquista della modernità, ma pubblicità del giudizio non deve significare gogna mediatica, non delocalizzazione della scena giudiziaria sul web che è, invece, quanto spesso rischia di avvenire per effetto della sostituzione del processo "mediatico" a quello "istituzionale", sin dalle fasi delle indagini. Così, spesso, la gogna mediatica costituisce un "fine pena mai" a prescindere da come si concluda il processo". Il tema intercettazioni, ha concluso Soro, risulta essere "sempre divisivo e di difficile trattazione, dovendosi trovare il punto di equilibrio tra esigenze investigative, diritto di difesa e riservatezza delle parti e dei terzi coinvolti,

come anche il diritto di informazione. Non è facile tracciare con nettezza la distinzione tra il giornalismo d'inchiesta e il "giornalismo di trascrizione o di riporto" spesso tanto superfluo ai fini informativi quanto dannoso per la riservatezza degli interessati".

Il 26 settembre, al 2° forum nazionale dei commercialisti ed esperti contabili "Come la rivoluzione digitale sta cambiando la professione", Giovanna Bianchi Clerici, componente del Garante, è intervenuta sugli adempimenti in materia di *privacy* ed antiriciclaggio illustrando, in particolare, il principio di *accountability* e le misure da adottare per l'attuazione del RGPD ed assicurare la sicurezza dei dati.

Per il tredicesimo anno consecutivo Consumer's forum ha organizzato l'incontro, tenutosi a Roma il 22 novembre, con le maggiori autorità amministrative indipendenti italiane. L'incontro è stato dedicato al tema "Il cittadino nell'era dell'algoritmo" ed ha affrontato temi centrali quali gli *smart meters*, l'internet delle cose, la *blockchain*; la *data driven innovation*; le imprese Fintech e i problemi di regolamentazione. La prof. Califano – componente del Garante – è intervenuta trattando il tema della tutela della protezione dati quale elemento di garanzia e sviluppo regolato nel mercato digitale.

L'11 dicembre si è tenuto l'incontro organizzato da Altroconsumo presso la Camera dei deputati a Roma, dal titolo "2018-2019 *data protection*: un biennio rivoluzionario". Il presidente Soro ha affrontato il tema della preoccupante tendenza a contrarre il diritto alla protezione dati per esigenze di mercato e ha affermato che la protezione dei dati si caratterizza sempre più quale tecnica di libertà, strumento di limitazione dei poteri altrimenti soverchianti, baricentro attorno a cui la tutela della persona e lo sviluppo dell'economia digitale possono incontrare una sintesi lungimirante.

Nel 2018 al presidente Soro è stato assegnato il "Premio Vincenzo Dona, voce dei consumatori" per la sezione "Personalità". La motivazione ha sottolineato come il Garante abbia svolto "con ancora maggiore impegno, il suo ruolo a difesa dei consumatori e del mercato, facendo sentire la sua voce anche verso il legislatore nel contrasto a fenomeni quali il telemarketing scorretto e l'approvazione della legge sui *call center*". All'Autorità è stato dunque riconosciuto il ruolo fondamentale di arbitro tra tutti i soggetti del mercato sia consumatori che imprese.

Il premio è stato istituito dall'Unione nazionale consumatori, a partire dal 2007, per ricordare il suo fondatore e premiare il lavoro svolto a favore dei consumatori da parte del mondo della politica, delle istituzioni, della società civile, del giornalismo, della ricerca universitaria. La manifestazione si fregia della Medaglia di rappresentanza del Presidente della Repubblica italiana e si svolge ogni anno con il patrocinio della Presidenza del Consiglio dei ministri, del Ministero dello sviluppo economico e del Ministero delle politiche agricole alimentari e forestali**.** L'edizione 2018 è stata dedicata al tema: "L'intelligenza dei dati".

24.5. *L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi*

Anche nel 2018 l'Ufficio relazioni con il pubblico, fondamentale strumento con cui il Garante svolge il compito di promozione della consapevolezza del pubblico (interessati, ma anche titolari e responsabili del trattamento), è stato impegnato in maniera intensa e costante nello svolgimento delle diverse attività cui è preposto: consulenza ai visitatori in sede, assistenza telefonica, gestione delle numerosissime richieste pervenute via e-mail (cfr. sez. IV, tab. 14 e 15).

L'anno di riferimento è stato caratterizzato da un sostanziale aumento delle

richieste pervenute all'Urp, soprattutto a ridosso del 25 maggio, data in cui il RGPD è divenuto direttamente applicabile nella UE. Oggetto della maggior parte delle stesse è stata proprio la nuova normativa: si pensi che nel solo mese di maggio più di 1.600 e-mail hanno riguardato i nuovi adempimenti sanciti dal RGPD.

L'Ufficio ha costantemente fornito la propria assistenza, come negli anni precedenti, garantendo al tempo stesso approfondita e aggiornata conoscenza giuridica delle questioni sottoposte, cortesia e tempestività nella risposta. Esso si conferma nel suo importante ruolo di primo interlocutore dell'Autorità verso l'esterno, cosa che gli consente di cogliere in tempo reale le problematiche più rilevanti e trasferirle, anche tramite *report* interni, alle altre unità organizzative.

L'Urp, in collaborazione con gli altri uffici interessati, ha curato la predisposizione di FAQ relative alla procedura telematica per la comunicazione dei dati del Rpd, fornendo poi la propria continua assistenza sia ai titolari e responsabili del trattamento sia agli stessi soggetti nominati Rpd.

Nel 2018 l'Urp ha gestito un numero particolarmente cospicuo di richieste (oltre 22.800), delle quali circa 16.000 (contro le 10.900 dello scorso anno, con un incremento di circa il 47%) pervenute via e-mail. Fermo restando l'inevitabile incremento dei quesiti dovuto all'applicazione del nuovo RGPD, tali dati confermano l'importanza ormai consolidata delle tematiche concernenti la *data protection* presso l'opinione pubblica, nonché la fiducia della stessa nei confronti del Garante. Circa 380 sono stati gli affari definiti (contro i 300 dello scorso anno, con un incremento di circa il 27%) e 360 i visitatori ricevuti in sede (contro i 200 dello scorso anno, con un incremento dell'80%).

Tematiche d'interesse

Le questioni sottoposte all'Urp nel 2018, soprattutto nella seconda parte dell'anno, sono state molteplici. Si segnalano di seguito quelle di maggiore interesse.

Il più alto numero di richieste di chiarimento ha avuto ad oggetto i nuovi adempimenti introdotti dal RGPD (oltre 4.300 e-mail): i nuovi principi di minimizzazione dei dati e di *accountability*, la designazione del Rpd, la valutazione di impatto e la tenuta dei registri delle attività di trattamento, la sicurezza dei dati. Altrettante istanze, pervenute soprattutto da imprese e pubbliche amministrazioni, hanno avuto ad oggetto il rapporto tra le disposizioni del RGPD e gli articoli del Codice relativi ad ambiti non direttamente interessati dalla modifica normativa, soprattutto in seguito all'entrata in vigore del decreto legislativo n. 101/2018, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del RGPD. Moltissime richieste hanno riguardato il rapporto tra titolari e responsabili del trattamento di cui all'art. 28 del RGPD, con particolare riferimento alla definizione del ruolo, delle competenze e delle responsabilità da attribuire ad alcune specifiche figure quali il medico competente e i consulenti del lavoro. Molti professionisti, in particolare, si sono rivolti all'Urp dopo che il Consiglio nazionale dei consulenti del lavoro ha adottato la circolare 23 luglio 2018, n. 1150, nella quale ha sostenuto che i consulenti in questione, nelle attività di trattamento dei propri clienti e dei dipendenti di questi ultimi, assumono la qualifica di titolare del trattamento o, al più, di co-titolari. Al riguardo, il Garante ha invece chiarito, con una nota al Consiglio del 22 gennaio 2019 (doc. web n. 9080970), che i consulenti debbano essere identificati come responsabili del trattamento quando trattano i dati dei dipendenti dei clienti in base all'incarico da questi ricevuto.

Anche se in numero minore rispetto all'anno precedente, il telemarketing aggressivo continua ad essere fonte di grande disturbo per i cittadini, che si sono rivolti all'Urp con circa 1.480 e-mail. Sono stati inoltre chiesti chiarimenti in ordine alle novità introdotte in materia dalla legge 11 gennaio 2018, n. 5, rispetto alla quale

tuttavia si è ancora in attesa del regolamento attuativo previsto dall'art. 1, comma 15 della legge stessa, al fine di modificare e integrare il d.P.R. n. 178/2010.

Sostanzialmente coincidenti a quelle dello scorso anno sono state, invece, le richieste concernenti il marketing via sms, fax e e-mail (circa 860 e-mail), come pure quelle relative alle attivazioni di servizi a pagamento non richiesti sulle utenze di telefonia mobile effettuate nel corso della navigazione in internet, nonché all'accesso ai dati di traffico telefonico e telematico.

Sempre di grande attualità – e quindi oggetto di innumerevoli richieste (circa 640 e-mail) – è il tema della videosorveglianza sia in ambito privato sia in ambito pubblico, in particolare con riguardo all'installazione dei sistemi di videosorveglianza negli asili nido e nelle scuole dell'infanzia, nelle strutture socio-sanitarie e socio-assistenziali per anziani e persone con disabilità.

Nell'anno trascorso si registra un notevole aumento dell'interesse suscitato dalle questioni concernenti i trattamenti di dati personali in internet e nei *social network* (più di 1.000 e-mail a fronte delle 780 circa dello scorso anno), in modo particolare con riferimento alle richieste di deindicizzazione dei dati personali dai motori di ricerca.

Molte richieste di chiarimento hanno riguardato, soprattutto verso la fine dell'anno, i nuovi adempimenti concernenti la fatturazione elettronica, con particolare riferimento ai soggetti che erogano prestazioni sanitarie, espressamente esonerati dall'obbligo di emissione a seguito del provvedimento del Garante 20 dicembre 2018, n. 511 (doc. web n. 9069072).

Altra questione oggetto di interesse è stata quella relativa al regime di accessibilità delle liste elettorali a seguito dell'abrogazione, ad opera del decreto legislativo n. 101/2018, dell'art. 177, d.lgs. n. 196/2003, in particolare del comma 5 che aveva modificato l'art. 51, d.P.R. n. 223/1967 introducendo delle restrizioni alla possibilità di avere copia delle liste stesse.

Più numerose rispetto all'anno passato sono state anche le richieste di chiarimenti relative al contesto lavorativo (più di 520 e-mail a fronte delle 350 circa del 2017), soprattutto per ciò che concerne l'uso di internet e della posta elettronica sul posto di lavoro, il trattamento degli indirizzi di posta elettronica a seguito della cessazione del rapporto di lavoro, il trattamento dei dati sensibili correlato al riconoscimento di permessi o benefici, l'uso di sistemi di rilevazione biometrica sul posto di lavoro.

25 Studi, documentazione e biblioteca

25.1. *Il Servizio studi e documentazione*

Relazione annuale

Al fine di dare attuazione ad uno degli adempimenti rilevanti che la legge pone in capo al Garante (cfr. art. 154, comma 1, lett. *e*), del Codice nonché l'art. 59 RGPD) – quello di dare conto dell'attività svolta al Parlamento e al Governo –, il Servizio studi e documentazione ha continuato a svolgere una funzione di coordinamento nella predisposizione del testo della Relazione annuale sull'attività svolta nel 2017 e sullo stato di attuazione del Codice. La pubblicazione sul sito istituzionale del Garante della Relazione consente inoltre di perseguire una più ampia finalità di trasparenza sull'attività svolta dall'Autorità non soltanto rispetto ai soggetti destinatari *ex lege* della stessa, ma anche nei confronti dell'intera collettività, rappresentando in pari tempo un prezioso strumento di conoscenza per diverse categorie di utenti a vario titolo interessati all'applicazione della disciplina in materia di protezione dei dati personali. In questa prospettiva, la struttura della Relazione, che presenta tradizionalmente una parte generale e molteplici sezioni tematiche (ivi comprese quelle contenenti informazioni di natura statistica), consente di fornire, in modo rapido e sintetico, informazioni puntuali sull'attività svolta (con particolare riguardo all'attività provvedimentale, sanzionatoria e comunicativa, nonché a quella svolta in ambito europeo ed internazionale) ed aggiornamenti su specifici profili o istituti attinenti alla protezione dati.

A ciò si aggiunga che, come è noto, in conformità a quanto previsto dall'art. 22, d.l. n. 90/2014 convertito in legge 11 agosto 2014, n. 114, la Relazione (non diversamente da quella delle altre autorità amministrative indipendenti) viene altresì trasmessa alla Corte dei conti (attività che con regolarità è stata assolta dal 2014).

Attività di studio, documentazione e supporto giuridico

Studi e ricerche sono state condotte su molteplici questioni tecnico-giuridiche di attualità nonché su materie di interesse dell'Autorità. L'attività di documentazione viene svolta mediante il costante monitoraggio della giurisprudenza, dottrina e documentazione nazionale, comunitaria ed internazionale, in particolare in materia di protezione dati, con la predisposizione di un osservatorio ad uso interno nonché con approfondimenti su questioni o settori specifici: in tale prospettiva hanno formato oggetto di esame (anche in prospettiva applicativa) le innovazioni legislative apportate alla legge 6 novembre 2012, n. 190, novellata dalla legge 30 novembre 2017, n. 179, in relazione alle tutele del dipendente che segnala illeciti (cd. *whistleblowing*). Approfondimenti sono stati effettuati in vista dell'articolata e complessa attività di revisione dei regolamenti sulle procedure interne nn. 1 e 2 del 2007 resa necessaria dalle innovazioni introdotte dal RGPD sull'attività dell'Autorità.

Il Servizio ha inoltre fornito il proprio supporto in relazione all'indagine congiunta, svolta dal Garante unitamente all'Agcom e l'Agcm, in materia di *big data*, finalizzata all'individuazione di eventuali criticità connesse all'utilizzo degli stessi, anche nella prospettiva della definizione di un quadro di regole in grado di promuovere e tutelare la protezione dei dati personali, la concorrenza dei mercati dell'economia digitale, la tutela del consumatore, nonché i profili di promozione del pluralismo nell'ecosistema digitale (cfr. in merito doc. web n. 6441412).

25.2. *La biblioteca*

La biblioteca è nata nel 2001 per raccogliere, organizzare, classificare con criteri bibliografici, conservare, gestire e valorizzare le pubblicazioni italiane e straniere attinenti alla disciplina della protezione dei dati nonché alle tematiche dei diritti e delle libertà fondamentali, della dignità, della riservatezza e della identità personale.

Nel contesto generale di prosecuzione della razionalizzazione della spesa (v. già Relazione 2017, p. 190) e di predisposizione delle operazioni di trasloco nella nuova sede, il ricco patrimonio della biblioteca – una singolarità a livello italiano ed europeo, atteso che il Garante risulta unico nella UE ad avere istituito una biblioteca multilingue, specializzata sui temi della *privacy* e della protezione dei dati, di grandi dimensioni (la cui composizione, nel dettaglio descritta nelle precedenti Relazioni, comprende 29.000 stampati, con ca. 15.000 monografie, opuscoli ed estratti di pubblicazioni, 7.500 dei quali in lingua straniera, ed è arricchita da Fondi speciali, donati dal prof. Rodotà e dal cons. Buttarelli) – è stato temporaneamente trasferito in magazzini, in vista del riallestimento di una o più sale di lettura e di consultazione.

La biblioteca supporta altresì le attività di informazione, di ricerca e di studio dell'Autorità; i servizi all'utenza esterna sono pertanto complementari (anche in ragione delle risorse disponibili) rispetto a questo fine istituzionale. Nel 2018 i servizi all'utenza interna ed esterna hanno funzionato in modo ridotto a causa del nuovo trasloco e dei trasferimenti delle collezioni nei magazzini. La consultazione del catalogo Opac sulla intranet ha registrato 1.430 contatti. Per quanto riguarda i *database* giuridici gestiti sulla intranet attraverso il sito web della biblioteca, i dati di consultazione da parte dei dipendenti dell'Autorità rivestono speciale importanza come indicatori dell'elaborazione che precede la messa a punto dei "prodotti" dell'Ufficio. Anche in questo caso le esigenze di una razionalizzazione della spesa hanno imposto tuttavia una revisione delle banche dati a disposizione dei dipendenti dell'Autorità. Il *database* con il più elevato conteggio ha registrato 8.201 sessioni di lavoro (7.892 nel 2017, 7.516 nel 2016, 6.864 nel 2015, 6.814 nel 2014, 6.529 nel 2013, 5.828 nel 2012, 4.889 nel 2011 e 4.052 nel 2010) e 94.920 documenti consultati (93.556 nel 2017, 89.103 nel 2016, 75.147 nel 2015, 83.831 nel 2014, 75.525 nel 2013, 60.419 nel 2012, 60.141 nel 2011 e 48.112 nel 2010), per una media giornaliera lavorativa di ca. 37 connessioni e 431 documenti (36 connessioni e 425 documenti nel 2017, 34 connessioni e 405 documenti nel 2016, 30 connessioni e 326 documenti nel 2015, 30 connessioni e 364 documenti nel 2014, 28 connessioni e 337 documenti nel 2013).

L'Ufficio del Garante

III - L'Ufficio del Garante

26 La gestione amministrativa e dei sistemi informatici

26.1. *Il bilancio e la gestione economico-finanziaria*

La gestione amministrativa dell'Autorità è stata improntata al rispetto dei principi di prudente valutazione delle entrate e di una attenta programmazione delle spese, nell'osservanza delle procedure e dei vincoli contenuti nelle disposizioni legislative e regolamentari applicabili al Garante.

L'esercizio 2018 è stato caratterizzato da una significativa revisione del finanziamento dell'Autorità attraverso interventi legislativi che hanno interessato l'entità delle risorse stanziate, anche al fine di consentire una migliore programmazione delle attività istituzionali.

Il legislatore, infatti, in ragione dei compiti previsti nell'ambito del RGPD ed al fine di assicurare il regolare esercizio dei poteri di controllo affidati al Garante, già con la legge 20 novembre 2017, n. 167, recante disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea, ha disposto un potenziamento dell'organico dell'Autorità, con la conseguente previsione di risorse finanziarie aggiuntive per un ammontare di oltre 4 milioni di euro, i cui effetti si sono manifestati a valere soprattutto dall'anno 2018.

Con legge 27 dicembre 2017, n. 205 (legge di bilancio 2018) si è provveduto ad assicurare ulteriore stabilità all'assetto gestionale dell'Autorità, con la previsione di finanziamenti a regime per complessivi 2 milioni di euro dal 2018 ed ulteriori 4 milioni di euro dal 2019. La rimodulazione dell'entità del finanziamento ha di fatto consentito un miglioramento dell'attività di programmazione della spesa e di proficuo impiego delle risorse.

Sotto il profilo della spesa, l'esercizio finanziario si è svolto assicurando la regolare esecuzione delle ordinarie attività gestionali, nonché l'espletamento di incombenze di carattere straordinario, tra le quali vanno annoverate quelle di particolare rilievo, anche a fini organizzativi, connesse al trasloco degli uffici presso la nuova sede di piazza Venezia. La necessità di accorpare in un'unica sede gli uffici dell'Autorità, dislocati in precedenza per esigenze di spazio in due diverse strutture, ancorché contigue, ha comportato la necessità di affrontare oneri di carattere straordinario connessi al trasloco e all'adeguamento degli spazi.

Riguardo alle specifiche esigenze di contenimento delle spese di gestione, l'Autorità ha continuato a porre in essere tutti gli opportuni adempimenti per gestire i propri servizi logistici con criteri di economicità, nel rispetto delle vigenti prescrizioni.

Come per il passato, l'Autorità non detiene immobili adibiti ad abitazione o foresteria.

Nel corso dell'esercizio non sono stati conferiti incarichi di studio e di consulenza, ex art. 5, d.P.R. n. 338/1994.

La gestione amministrativa del Garante è stata assoggettata agli ordinari e periodici controlli dell'organo preposto alla verifica della regolarità amministrativo-contabile e nel corso dell'esercizio non sono state riscontrate irregolarità, né sono stati formulati rilievi.

Sotto il profilo più strettamente contabile, il risultato finanziario dell'esercizio ha fatto registrare un importante avanzo di amministrazione, pari a oltre 3,5 milioni di euro, il cui risultato è ascrivibile, oltre che ad un'oculata gestione della spesa, all'accelerazione dell'acquisizione delle entrate rispetto alla tempistica occorrente per la programmazione ed il perfezionamento delle uscite che risulta naturalmente dilatata allorquando il relativo procedimento non si esaurisce in tempi brevi. Ed infatti, la necessità di acquisire nuovo personale e la concreta immissione in ruolo dei dipendenti richiede l'espletamento di lunghe ed articolate procedure che incidono ai fini del disallineamento temporale tra il momento dell'acquisizione delle risorse finanziarie, che risulta anticipato e definito in prossimità dell'inizio dell'esercizio finanziario, ed il loro effettivo impiego, che si concretizza con l'adozione del relativo provvedimento di assunzione, ragionevolmente dopo un lasso di tempo significativo che può prolungarsi anche oltre l'esercizio finanziario in corso.

Nel corso del 2018, al netto delle partite di giro, le entrate complessivamente acquisite dall'Autorità sono state pari a 26,9 milioni di euro a fronte delle quali sono stati registrati impegni di spesa per 23,4 milioni di euro. Le risorse finanziarie acquisite al bilancio del Garante sono rappresentate, per la quasi totalità di esse, da trasferimenti erariali disposti nell'ambito della pertinente legge di bilancio. Infatti, le risorse finanziarie trasferite dal bilancio dello Stato sono state pari a 26,6 milioni di euro, il cui importo raccoglie le previsioni dei diversi provvedimenti legislativi che si sono concentrati soprattutto negli anni più recenti per assicurare che la programmazione delle attività potesse tenere conto delle incombenze introdotte dal RGPD.

La somma complessivamente trasferita per le esigenze di funzionamento è comprensiva dell'importo, nella misura del 50%, delle sanzioni irrogate dal Garante per le violazioni delle disposizioni in materia di protezione dei dati personali, i cui proventi sono versati dai debitori per l'intera entità direttamente nelle casse erariali e solo successivamente sono riassegnate al Garante nella misura di legge spettante.

Ulteriori entrate di carattere marginale, pari a 0,3 milioni di euro, sono imputabili a diritti di segreteria ed a rimborsi di varia natura. Peraltro i proventi da diritti di segreteria sono destinati ad esaurirsi in ragione di una puntuale disposizione contenuta nel RGPD che prevede da parte delle singole autorità nazionali lo svolgimento dei propri compiti senza spese né per l'interessato né, ove applicabile, per il titolare del trattamento.

Dalla tabella 18 (cfr. sez. IV) si evince un significativo incremento delle entrate correnti rispetto al corrispondente valore del precedente esercizio finanziario, ascrivibile alle misure legislative intervenute a sostegno dell'attività istituzionale dell'Autorità (+5,9 mil. di euro, pari a +27,85%).

La spesa complessiva fa registrare un significativo incremento rispetto ai valori del precedente esercizio (+4,0 mil. di euro, pari a +20,73%), anche se in termini assoluti è di entità più contenuta rispetto all'incremento delle entrate in quanto una parte significativa di essa, essendo destinata all'incremento dell'organico, come anticipato richiede tempi più dilatati per l'assunzione dei relativi oneri a carico del bilancio.

In generale, anche per il 2018, la struttura della spesa si caratterizza, come per

la generalità di analoghi soggetti pubblici, per una significativa incidenza degli oneri del personale, le cui risorse, tuttavia, rappresentano per esperienza, competenza e professionalità un fattore di primaria importanza nello svolgimento delle innumerevoli funzioni che l'Autorità è chiamata ad espletare, sia in ambito nazionale, sia attraverso una costante partecipazione nelle pertinenti sedi istituzionali europee.

L'indennità di carica dei componenti del Garante non ha subito variazioni rispetto al precedente esercizio ed il loro importo è rimasto contenuto entro i prescritti limiti di legge.

Con riferimento, infine, agli oneri strettamente connessi alle esigenze gestionali, nel corso dell'anno risultano in generale rispettati i prescritti limiti.

26.2. *L'attività contrattuale, la logistica e la manutenzione dell'immobile*

Attività contrattuale

L'attività dell'Autorità concernente i contratti pubblici è proseguita, in linea con gli obiettivi del Garante e nel rispetto della normativa vigente, secondo la quale le autorità amministrative indipendenti, al fine di dare attuazione alle esigenze di razionalizzazione, sono tenute a gestire "i servizi strumentali in modo unitario, mediante la stipula di convenzioni o la costituzione di uffici comuni ad almeno due organismi" (cfr. art. 22, d.l. 24 giugno 2014, n. 90, convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 11 agosto 2014, n. 114).

Entro questa cornice sono state aggiudicate due procedure di gara di rilevanza comunitaria: la prima, gestita in comune con l'Arera nonché con l'Autorità di regolazione dei trasporti, relativa al programma di assistenza sanitaria e malattia; la seconda, con l'Agcom e con l'Autorità di regolazione dei trasporti, relativa ad ulteriori servizi assicurativi (sede, patrimonio mobiliare, responsabilità civile, ecc.), all'esito della quale sono stati stipulati i contratti per i quattro lotti di interesse del Garante.

Sono stati altresì ampiamente utilizzati, come già in passato, gli strumenti messi a disposizione da Consip s.p.a. sul portale Acquistinretepa.it, oltre alle convenzioni, è stato utilizzato lo strumento del contratto quadro e sono stati realizzati numerosi acquisti a mezzo Richiesta di offerta (Rdo), Trattativa diretta (Td) ed Ordine diretto d'acquisto (Oda) sul Mercato elettronico della p.a. (Mepa). In particolare, il Garante ha aderito al contratto quadro Consip denominato "Spc *cloud*" - lotto n. 4, avente ad oggetto i servizi di realizzazione e gestione di portali e servizi *online*, stipulato anche al fine di accrescere il livello qualitativo dei servizi *online* dell'Autorità, sia in relazione ai compiti e agli adempimenti connessi alla previgente normativa, sia in relazione all'applicazione del RGPD, dal quale sono derivati accresciuti obblighi di comunicazione nei confronti dell'Autorità.

Con adesione alle convenzioni Consip sono stati stipulati i contratti di fornitura del servizio sostitutivo di mensa mediante buoni pasto elettronici nonché la fornitura di energia elettrica.

Tra le procedure svolte tramite Rdo sul Mepa, si segnalano quella avente ad oggetto il servizio trasloco degli uffici presso la nuova sede che ha comportato complesse attività e la Rdo concernente il servizio di rassegna stampa nonché altri servizi parzialmente innovativi (ad es., il monitoraggio web).

Con riferimento alle previsioni di cui alla legge di stabilità 2016 (art. 1, comma 512, l. 28 dicembre 2015, n. 208), si evidenzia che tutti gli acquisti di *hardware* e *software* sono stati effettuati utilizzando i summenzionati strumenti di acquisto e negoziazione del portale Consip. Le acquisizioni hanno riguardato, in particolare, i

beni e i servizi necessari alla prosecuzione delle attività dell'Ufficio presso la nuova sede (servizi di telefonia e connettività, materiali per la sala Ced, ecc.), nonché ulteriori beni e servizi concernenti la normale operatività dell'Autorità, quali ad esempio la fornitura di *software* gestionali di normale utilizzo o l'acquisizione di taluni arredi per la nuova sede.

Logistica e manutenzione dell'immobile

Nel 2018 la logistica e la manutenzione dell'immobile ha comportato un'attività particolarmente intensa in quanto, all'esito di attività pluriennali, è stata individuata la nuova sede dell'Autorità in piazza Venezia, presa in locazione da Generali s.p.a., stante l'indisponibilità di immobili demaniali o comunque pubblici. Le superfici acquisite, pur se paragonabili in termini assoluti con quelle precedentemente utilizzate (in due sedi distinte), risultano tuttavia più razionali e fruibili, sì da consentire anche l'allocazione di un maggior numero di unità – tenendo conto delle implementazioni dell'organico effettuate, nonché di quelle future – oltre ad un miglioramento del rapporto mq/addetti.

Nel corso della parte finale del 2018 sono state in parte effettuate, ed in parte avviate, talune attività di miglioramento funzionale della nuova sede da parte della società proprietaria. Il trasloco nella nuova sede ha poi consentito all'Ufficio di avviare la predisposizione degli atti di autonome procedure di gara relative ai servizi necessari, stante la perdurante indisponibilità della convenzione Consip "*Facility management* 4"; nelle more dell'espletamento di tali procedure di gara, si è proceduto – al pari di altre Amministrazioni e Autorità indipendenti – alla proroga del vigente contratto, stipulato in adesione alla precedente convenzione Consip "*Facility management* 3", per il periodo di sei mesi.

26.3. *L'organizzazione dell'Ufficio*

Il personale ed i collaboratori esterni

Le novità introdotte dal RGPD nonché dal decreto legislativo n. 101/2018 hanno comportato un ampliamento dei compiti istituzionali del Garante e quindi un impatto significativo sulla struttura dell'Ufficio, tanto che nel corso dell'anno di riferimento è stata attuata un'importante riorganizzazione dell'Autorità che ha visto ridisegnare la composizione di alcune unità organizzative, ridefinendone le competenze (provv. 22 febbraio 2018, n. 118, doc. web n. 7896186).

Nel 2018 è stata espletata una procedura concorsuale finalizzata alla copertura di otto posti di funzionario con profilo giuridico-amministrativo conclusasi con l'approvazione della graduatoria di merito e l'immissione dei vincitori nel ruolo organico del Garante.

Con riguardo alla convenzione quadro in materia di procedure concorsuali congiunte per il reclutamento del personale delle autorità indipendenti siglata nel 2015 ai sensi dell'art. 22, comma 4, d.l. n. 90/2014, sono state bandite da altre autorità indipendenti alcune procedure concorsuali alle quali tuttavia il Garante, in ragione della specificità dei profili richiesti, non ha ritenuto di aderire, attivando a sua volta tre procedure di mobilità volontaria esterna ai sensi dell'art. 30, d.lgs. n. 165/2001, rispettivamente per due posti di dirigente giuridico-amministrativo, un posto di dirigente giuridico-internazionale e quattro posti di impiegato operativo provvedendo ad effettuare, nel rispetto della citata convenzione quadro, le relative comunicazioni alle altre autorità.

Al 31 dicembre 2018 l'Ufficio poteva così contare su un organico di 162 unità, di cui 120 in servizio, al quale va aggiunto un contingente di 8 unità a contratto a tempo determinato, di cui 5 in servizio (cfr. sez. IV, tab. nn. 16 e 17).

Sono state espletate due procedure semestrali per la selezione di giovani laureati

per l'effettuazione di tirocini presso l'Autorità cui si è registrata un'elevata partecipazione ed è stato avviato per la prima volta un progetto di *visiting*, patrocinato dalla Regione Lazio.

Con riferimento agli adempimenti previsti dal decreto legislativo n. 81/2008 in materia di tutela della salute e della sicurezza nei luoghi di lavoro, sulla base della convenzione Consip attivata a copertura del triennio 2016/2019, l'Ufficio, coadiuvato dal Responsabile del servizio prevenzione e protezione (Rspp) e con l'ausilio dei preposti della società locatrice Generali s.p.a., ha provveduto ad adeguare tutta la documentazione sulla sicurezza in relazione alla nuova sede di piazza Venezia, con particolare riguardo al documento di valutazione dei rischi (dvr).

Tenuto conto che le attività di formazione obbligatoria si sono concluse nel primo semestre 2018, l'Ufficio ha svolto, con l'ausilio del Rspp e dell'impresa aggiudicataria del servizio di gestione di sicurezza integrata (Exitone s.p.a., oggi GIone s.p.a.), alcune attività di programmazione, per il primo semestre 2019, riguardanti la formazione dei nuovi assunti, dei futuri stagisti e di altre eventuali attività di interesse per l'Autorità.

Le attività di formazione si sono svolte avvalendosi dell'offerta della Scuola nazionale dell'amministrazione (Sna), il cui catalogo è in continuo aggiornamento anche grazie al lavoro svolto dal Club dei formatori della Scuola, progetto al quale l'Autorità partecipa che nasce per implementare metodi e materie su cui elaborare piani formativi che si attaglino sempre meglio alle esigenze della p.a.

Parte rilevante del personale ha usufruito dei corsi Sna con particolare riguardo alla formazione obbligatoria nelle materie dell'anticorruzione (cfr. par. 26.4), della normativa appalti e contratti e del *whistleblowing*.

Collaboratori esterni

Presso l'Autorità continua ad operare il servizio di controllo interno, presieduto da un magistrato della Corte dei conti e composto da due dirigenti generali, rispettivamente della Ragioneria generale dello Stato e della Presidenza del Consiglio dei ministri.

Segreteria generale

Nel periodo di riferimento, l'attività del Garante è stata improntata al metodo della programmazione e sul rispetto dei principi di economicità ed efficienza dell'azione amministrativa, in conformità al Regolamento n. 1/2000 sull'organizzazione e il funzionamento dell'Ufficio, attraverso l'attività di coordinamento svolta dal Segretario generale, soggetto preposto all'Ufficio ai sensi dell'art. 156, comma 1, del Codice.

Il corretto espletamento da parte del Garante dei compiti e dei poteri attribuiti dalla disciplina vigente è stato garantito dal Segretario generale attraverso il raccordo tra le Unità organizzative e il Collegio, la costante attività istruttoria degli schemi di provvedimento oggetto di esame nel 2018 (per un totale di circa cinquanta adunanze), la partecipazione a diversi incontri e innumerevoli interlocuzioni con attori istituzionali e organismi rappresentativi di varie categorie, svolti anche in ambito internazionale ed europeo. Ciò ha consentito, sia di mettere a disposizione, in consessi istituzionali internazionali, l'esperienza maturata dall'Autorità, anche allo scopo di consolidare le linee istituzionali assunte sulle tematiche di maggiore criticità in relazione alla protezione dei dati personali; inoltre, il costante confronto e l'aggiornamento hanno permesso di riportare nell'Ufficio le buone prassi sviluppate all'estero.

In tale quadro, si segnala, in particolare, la partecipazione del Segretario generale ai lavori del Gruppo Art. 29 e, dal momento della sua istituzione, alle sessioni plenarie del Comitato europeo di protezione dati, nonché la partecipazione alla *Spring Conference* che si è tenuta a Tirana (2-5 maggio 2018), durante la quale ha presentato una relazione dal titolo "*Enhancing oversight cooperation in surveillance: the role*

of DPAs. The Italian Experience", nonché la partecipazione alla *International Conference of Data Protection and Privacy Commissioners* – Icdppc (22-26 ottobre 2018): in tale occasione, il Segretario generale ha partecipato alla tavola rotonda sul tema "*The concept of fairness in data protection*" organizzata dal *Centre for Information Policy Leadership* (Cipl).

Inoltre, la posizione del Garante è stata rappresentata dal Segretario generale in occasione di incontri, convegni e seminari aventi ad oggetto gli aspetti di maggiore criticità interpretativa e/o difficoltà applicativa emergenti dalla disciplina. Gli interventi hanno riguardato, fra i tanti, la persona digitale, la tutela dei consumatori, l'intelligenza artificiale, il Rpd, l'economia digitale e i *big data*, il *marketing* indesiderato, l'internet delle cose.

Si è altresì partecipato alla progettazione e istituzione del Comitato Fintech presso il Mef, in collaborazione con Consob, Banca d'Italia e AgID; è stato poi seguito lo sviluppo dell'incontro formativo organizzato con altre autorità nazionali di controllo nell'ambito del progetto T4DATA (in partenariato con la Fondazione Lelio e Lisli Basso-Issoco sul progetto di formazione in materia, approvato dalla Commissione europea, focalizzato sulla figura del Responsabile per la protezione dati).

Particolarmente rilevante è stata l'attività volta a consentire l'ottimale applicazione del RGPD e il miglior recepimento della direttiva (UE) 2016/680 mediante il decreto legislativo n. 51/2018.

Preliminarmente, si segnala la partecipazione del Segretario generale al Gruppo di lavoro, in qualità di osservatore e in rappresentanza del Garante, istituito presso il Ministero della giustizia, incaricato di provvedere alla ricognizione, all'analisi e all'approfondimento delle disposizioni, di matrice europea, al fine di provvedere alla predisposizione dei decreti legislativi di cui alla legge n. 163/2017 di delegazione europea 2016-2017, in modo da garantire il recepimento e adeguamento dell'ordinamento interno alle disposizioni europee in materia di protezione dei dati personali (d.m. 14 dicembre 2017). Sempre nell'ambito dell'imminente applicabilità del RGPD, sono state emanate indicazioni preliminari volte a favorire la corretta applicazione delle disposizioni del Regolamento medesimo, anche in raccordo con le disposizioni nazionali in materia (provv. 22 febbraio 2018, n. 121, doc. web n. 8080493), oltre a chiarire sia alcune disposizioni del Codice previgente non più compatibili con il nuovo quadro legislativo, come ad esempio quelle riguardanti i ricorsi al Garante (provv. 31 maggio 2018, n. 374, doc. web n. 8997237), sia quelle derivanti dalla rinnovata disciplina a seguito dell'adozione del decreto legislativo n. 101/2018, come nel caso della trattazione degli affari pregressi (provv. 27 settembre 2018, n. 455, doc. web n. 9047256). Inoltre si è preso parte agli incontri con delegazioni straniere di altre autorità di protezione dei dati, con i rappresentanti diplomatici e governativi di altri Stati europei ed extraeuropei ovvero di importanti gruppi imprenditoriali, oltre a curare i rapporti con le altre autorità indipendenti.

È stato dato impulso agli adempimenti stabiliti dalla disciplina europea ai quali il Garante, al pari di ogni titolare del trattamento, è assoggettato: si è quindi provveduto ad istituire il registro dei trattamenti e il registro interno delle violazioni (provv. 4 ottobre 2018, n. 463, doc. web n. 9051107), oltre ad adottare la lista nazionale dei trattamenti da sottoporre a valutazione di impatto (provv. 11 ottobre 2018, n. 467, doc. web n. 9058979). Si è provveduto altresì a supervisionare l'adozione della nuova modulistica (ad es., moduli per la comunicazione e la modificazione dei dati di contatto del Rpd; per la notificazione dei *data breach*; ecc.).

Le altre tematiche sulle quali si è focalizzata l'attività hanno riguardato, fra le altre, il *whistleblowing* si è infatti proceduto a perfezionare la procedura già prevista presso il Garante a tutela della riservatezza del segnalante, emanando, in collaborazione con il Rpct, istruzioni in ordine all'*iter* da seguire in caso di segnalazione, congiuntamente alla modulistica volta a facilitare la presentazione delle istanze (nota 14 dicembre 2018, doc. web n. 9067511).

Al fine di assicurare l'efficienza del Garante, sotto il profilo organizzativo, il Segretario generale ha provveduto altresì a gestire le problematiche riguardanti il personale, le risorse interne e strumentali, la contrattualistica, la digitalizzazione dell'Ufficio, e i rapporti con le altre autorità indipendenti nel quadro delle convenzioni stipulate sui servizi strumentali.

Segreteria del Collegio

La segreteria del Collegio ha continuato a seguire le attività dell'organo collegiale collaborando con gli uffici e dipartimenti dell'Autorità in relazione alla predisposizione e distribuzione della documentazione necessaria per le adunanze (concernente in particolare schemi di provvedimento, appunti e note), la redazione e conservazione dei verbali delle riunioni e la custodia degli originali degli stessi e delle deliberazioni adottate. Ha altresì assicurato il controllo puntuale dei testi deliberati dal Collegio in vista della loro pubblicazione sul sito istituzionale dell'Autorità.

La segreteria del Collegio ha contribuito a gestire le richieste di oscuramento e di deindicizzazione di alcuni atti dell'Autorità, formulati da interessati e da titolari del trattamento coinvolti a vario titolo in alcune istruttorie condotte dall'Autorità, in particolare con riferimento a esigenze di riservatezza riguardo a casi di segreto industriale o *know-how* tecnologico.

L'Ufficio, in un'ottica di efficientamento delle risorse e di maggiore celerità delle attività, nel corso dell'anno ha proseguito nell'utilizzo di modalità di trasmissione elettronica dei documenti predisposti per l'esame e l'approvazione da parte del Collegio, assicurando tempestività ed efficienza nonché risparmi, conformemente a quanto disposto dall'art. 15 del Regolamento n. 1/2000. In tale ambito l'attività svolta consentirà di poter allineare in breve tempo le attività della segreteria del Collegio alle indicazioni contenute nel decreto legislativo n. 217/2017 che ha modificato il decreto legislativo n. 82/2005 (Cad) e al rispetto dei principi ispiratori della richiamata normativa.

Controllo di gestione

L'efficienza dell'Autorità è stata perseguita anche attraverso il controllo di gestione, che ha comportato un'analisi periodica degli affari assegnati alle diverse Unità organizzative, avvalendosi del nuovo sistema di protocollazione *Archiflow* implementato nel corso dell'anno, di una reportistica mensile di carattere statistico, che si è focalizzata sull'andamento della trattazione degli affari, il riepilogo dei flussi (fascicoli assegnati ed evasi) e il controllo delle pratiche esposte al rischio di arretrato.

Il Responsabile della protezione dei dati

Anche presso il Garante è stata istituita, nel corso dell'anno, la figura del Responsabile della protezione dei dati personali per lo svolgimento dei compiti indicati agli artt. 38 e 39 del RGPD.

26.4. *"Autorità trasparente" e adempimenti relativi alla disciplina anticorruzione*

Nel 2018 è stato adottato l'aggiornamento al Piano triennale di prevenzione della corruzione (Ptpc) per gli anni 2018-2020 redatto in conformità agli obiettivi programmatici indicati dal Garante (doc. web n. 7537114) e pubblicato sul sito istituzionale nella sezione Autorità trasparente (doc. web n. 7610948). Le misure gene-

rali e specifiche di prevenzione della corruzione previste dal Piano sono state attuate nel rispetto delle previsioni ivi contenute.

Si è proseguita l'attività formativa del personale dell'Autorità, limitatamente a quello maggiormente coinvolto nei processi a rischio corruzione, tramite i corsi organizzati dalla Scuola nazionale dell'amministrazione (Sna), tenendo conto delle risorse disponibili e delle complessive esigenze di funzionamento nonché dei carichi di lavoro gravanti sull'Autorità, in particolare a seguito dell'applicazione del RGPD.

Un'importante misura del Piano ha riguardato l'adozione di una procedura, comunicata a tutti i dipendenti e al personale operante presso il Garante nonché al Collegio e al Secin, di segnalazione di illeciti da parte dei dipendenti (*whistleblowing*) che prevede l'invio, a mezzo del servizio postale o *brevi manu*, della segnalazione di presunte condotte illecite al solo Rpct mediante un modello predisposto rinvenibile in formato elettronico sia sulla intranet che sul sito istituzionale nella sezione Autorità trasparente.

Con riguardo alla misura concernente la rotazione degli incarichi dirigenziali, a tale misura – strutturalmente già prevista dall'art. 9, comma 2, Regolamento del Garante n. 1/2000 – è stata data attuazione in fase di rinnovo degli incarichi dirigenziali.

Con riguardo alle istanze dirette all'Autorità volte ad esercitare il diritto di accesso civico – pari a trentasette nel 2018 –, il Rpct è stato chiamato a pronunciarsi in sede di riesame con riguardo a complessive diciannove trattazioni (diciotto delle quali riferite al 2018 ed una al 2017), fornendo a tutte un riscontro motivato, come previsto dalla legge; un'unica istanza di accesso civico si è incentrata invece su dati oggetto di pubblicazione obbligatoria (ai sensi dell'art. 5, comma 1, d.lgs. n. 33/2013), che non ha tuttavia dato luogo ad adeguamento perché le informazioni richieste risultavano già pubblicate.

Sono state predisposte e pubblicate sul sito del Garante sia la relazione annuale del Rpct per l'anno 2018 (art. 1, comma 14, l. n. 190/2012) relativa all'efficacia delle misure di prevenzione definite nel Ptpc 2018-2020 (doc. web n. 9079180) sia, nel rispetto del termine del 30 aprile 2018, la griglia di rilevazione di cui all'all. 2 della delibera Anac n. 141/2018, che il Rpct è tenuto a pubblicare in assenza di Oiv o strutture equivalenti presso l'Autorità.

Sempre in materia di trasparenza è stato inoltre fornito costante supporto a tutti gli uffici chiamati ad adempiere ad obblighi di pubblicazione.

26.5. *Il settore informatico e tecnologico*

Sviluppo del sistema informativo e dei servizi ICT

Nel 2018 l'attività di sviluppo del sistema informativo ha subito rallentamenti dovuti all'esigenza di fare fronte alla gestione di più sedi anche temporanee e a quella di fornire supporto nel corso del definitivo trasloco della sede del Garante.

Oltre alle normali attività di gestione dell'infrastruttura IT dell'Ufficio, è stato necessario avviare un percorso di convergenza verso la piena implementazione delle previsioni del Cad, il cui ambito di applicazione è stato di recente esteso alle autorità amministrative indipendenti.

È stato quindi stipulato un primo contratto esecutivo relativo alla convenzione Consip "SPC Lotto 4" per servizi e applicazioni web, nel cui ambito sono state acquisite le risorse per la realizzazione e l'erogazione di servizi *online* del Garante.

È stato messo in esercizio il nuovo sistema informatico di gestione del protocollo e dell'archivio, sostituendo il precedente in uso per quindici anni, che consente una

migliore integrabilità con le altre funzioni del sistema informativo grazie alla disponibilità di web *services* e alla rapidità di implementazione delle opportune interfacce.

In vista del trasferimento della sede dell'Autorità, sono state poste in essere tutte le opportune misure di carattere tecnico che hanno poi consentito, nell'ottobre 2018, di effettuare il trasferimento senza interruzioni dei servizi informatici e telefonici. Nell'ambito di questa fase sono stati riprogettati i sistemi di rete locale e telefonici ed è stata allestita una sala tecnica idonea a supportare le esigenze di connettività ed elaborazione dati dell'Autorità, contestualmente impegnata in un'azione di progressivo trasferimento dei sistemi applicativi verso soluzioni *cloud* per l'erogazione dei propri servizi.

Dati di contatto Rpd

Anche grazie alla disponibilità del nuovo sistema è stata sviluppata la procedura *online* per la comunicazione dei dati di contatto del Rpd prevista dall'art. 37, par. 7, del RGPD, che impone ai titolari e responsabili del trattamento che abbiano designato il Responsabile della protezione dei dati, di comunicarne i dati di contatto all'autorità di controllo.

Fin dai primi mesi del 2018 era stata avviata la progettazione di un sistema informatico destinato ad accogliere tali comunicazioni fornendo al contempo un riscontro immediato al soggetto che effettuava la comunicazione, oltre alla registrazione delle informazioni trasmesse all'interno delle altre componenti del sistema informativo dell'Autorità.

A partire dal 18 maggio 2018 è stata resa disponibile l'applicazione web mediante la quale è possibile ottemperare al citato obbligo di comunicazione.

Nei soli primi 10 giorni di attività di tale sistema è stato possibile accogliere circa 26.000 comunicazioni dei dati di contatto, la cui elaborazione manuale avrebbe invece richiesto un enorme impegno di risorse umane. Al 31 dicembre 2018, il numero delle comunicazioni di Rpd aveva raggiunto la cifra di 43.269 (27.935 soggetti privati e 15.334 soggetti pubblici).

Sicurezza informatica dell'Ufficio

Nel 2018 nessun evento relativo alla sicurezza ha prodotto danni o disservizi nel dominio dell'Ufficio. Non si sono registrate situazioni pregiudizievoli rispetto alla sicurezza informatica sulle postazioni individuali e sui sistemi *server*, né su altre componenti dell'infrastruttura.

La continuità dei servizi accessibili al pubblico (notificazione dei trattamenti e richieste di verifiche preliminari per gli istituti bancari) è stata in linea coi valori degli anni precedenti, con i valori di *downtime* dei servizi ancora gestiti *on premises* intorno alle dodici ore complessive nell'arco dell'anno per cause prevalentemente esterne, *black-out* elettrici di lunga durata, e solo in parte dovute a inevitabili fermi per consentire le operazioni di trasloco della sede dell'Autorità.

Attività di consulenza e cooperazione interna ed esterna

Le unità organizzative dell'Ufficio hanno cooperato assiduamente attraverso azioni di supporto e consulenza interna sulle tematiche di comune interesse e in base alle rispettive competenze: significativa in questo senso, in particolare, l'interazione con la componente tecnologica dell'Ufficio sui temi connessi all'innovazione digitale e alla sicurezza informatica, sia nell'ambito della trattazione di affari e procedimenti sia nel contesto dell'attività ispettiva.

In tal senso, significativo è stato l'impegno nel supporto tecnologico alla campagna ispettiva sul telemarketing, che ha comportato l'analisi di copiose moli di dati su chiamate indesiderate che ha consentito di rilevare e mettere a fuoco numerose irregolarità da parte di operatori di comunicazione elettronica poi oggetto di sanzioni, e il contributo fornito all'*audit* periodico nei confronti del Sistema nazionale di informazione visti (VIS), di cui alla decisione del Consiglio 2004/512/CE, finalizzato alla vigilanza sulla legittimità del trattamento dei dati personali dei richie-

denti il visto nonché nei confronti del sistema d'informazione Schengen di seconda generazione (SIS II), di cui al regolamento (CE) n. 1987/2006.

In sede di resa dei previsti pareri da parte dell'Autorità, la componente tecnologica dell'Ufficio ha contribuito al recepimento nell'ordinamento nazionale della direttiva (UE) 2016/680 (cd. *law enforcement directive*) e della direttiva (UE) 2016/681 (cd. *passenger name record directive*) e, per quanto riguarda lo sviluppo delle nuove tecnologie in ambito pubblico, ha fornito consulenza relativamente all'introduzione dell'obbligo di fatturazione elettronica tra privati (B2B e B2C) e alla gestione di banche dati di interesse nazionale, specialmente nell'ambito dell'istruzione, della sicurezza pubblica, della sanità e della fiscalità.

I dati statistici

IV - I dati statistici 2018

Tabella 1. Sintesi delle principali attività dell'Autorità

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	517
Pareri su provvedimenti normativi di rango primario	5
Pareri su atti regolamentari e amministrativi	23
Pareri ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	44
Autorizzazioni individuali al trattamento dei dati sensibili e giudiziari (art. 41, d.lgs. n. 196/2003)	5
Provvedimenti concernenti trasferimenti di dati consentiti verso Paesi terzi (art. 44, comma 1, lett. *a*), d.lgs. n. 196/2003)	3
Decisioni su ricorso (art. 145, d.lgs. n. 196/2003)	130
Provvedimenti collegiali su segnalazioni e reclami (artt. 142-144, d.lgs. n. 196/2003) nonché a seguito di accertamenti d'ufficio (art. 154, d.lgs. n. 196/2003) e ai sensi degli artt. 10, comma 2, 13, comma 5, lett. *c*), e 150, comma 5, d.lgs. n. 196/2003	72
Ordinanze-ingiunzione adottate dal Garante	159
Riscontri a segnalazioni, reclami, richieste di parere e quesiti (artt. 142-144, d.lgs. n. 196/2003 e artt. 5 e 11, Reg. Garante n. 1/2007)	5.640
Provvedimenti collegiali su verifiche preliminari per trattamenti che presentano rischi specifici (art. 17, d.lgs. n. 196/2003)	37
Comunicazioni al Garante su flussi di dati tra p.a. o in materia di ricerca scientifica (artt. 19, comma 2, 39 e 110, d.lgs. n. 196/2003)	8
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari	2
Ulteriori pareri resi a soggetti pubblici	12
Audizioni del Presidente del Garante o memorie scritte trasmesse al Parlamento	7
Risposte a quesiti e altre istanze	22.802
Leggi regionali esaminate	4
Rilievi formulati in relazione a leggi regionali ai fini dell'impugnazione da parte del Governo ex art. 127 Cost.	1
Accertamenti e controlli efffettuati *in loco* (artt. 157-158, d.lgs. n. 196/2003)	150
Violazioni amministrative contestate	707
Sanzioni applicate con ordinanza di ingiunzione	419
Pagamenti derivanti dall'attività sanzionatoria	8.161.806
Comunicazioni di notizia di reato all'autorità giudiziaria	27
Prescrizioni e verifiche di adempimento sulle misure minime di sicurezza (a fini di estinzione del reato)	13
Ricorsi (trattati) ex art. 152, d.lgs. n. 196/2003	16
Opposizioni (trattate) a provvedimenti del Garante	101
Notificazioni pervenute fino al 24 maggio 2018	779
Notificazioni pervenute dal 2004 al 24 maggio 2018	33.017
Comunicazioni dei dati di contatto dei Rpd	43.269
Istanze di accesso civico presentate al Garante, ai sensi dell'art. 5, comma 1, d.lgs. n. 33/2013	1
Istanze di accesso civico presentate al Garante, ai sensi dell'art. 5, comma 2, d.lgs. n. 33/2013	37
Istanze di riesame diniego accesso civico presentate al Rpct, ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	19
Riunioni del Gruppo Art. 29 / CEPD	7
Partecipazione a sottogruppi di lavoro - Gruppo Art. 29	59
Riunioni autorità comuni di controllo / organismi di supervisione (Europol, SIS II, Dogane, Eurodac, VIS)	11
Conferenze internazionali	2
Riunioni presso il CoE, OCSE e altri organismi internazionali	7
Riunioni e *workshop* presso Consiglio/Commissione e altri organismi UE	6
Altre conferenze e *meeting*	17

Tabella 2. Attività di comunicazione dell'Autorità

Attività di comunicazione dell'Autorità	
Comunicati stampa	38
Newsletter	12
Bollettino radiofonico del Garante	18
Prodotti editoriali	2
Prodotti web	7
Video *spot*	1

Tabella 3. Pareri ex art. 154, comma 4, d.lgs. n. 196/2003 e pareri ex art. 36, par. 4, del RGPD

Pareri ex art. 154, comma 4, d.lgs. n. 196/2003 e pareri ex art. 36, par. 4, del RGPD	
Temi	Riscontri resi nell'anno (*)
Attività di polizia, sicurezza nazionale e governo del territorio	8
Adeguamento normativa nazionale alle disposizioni del RGPD	1
Giustizia	4
Categorie particolari di dati	3
Fisco	6
Digitalizzazione della p.a.	3
Istruzione	1
Dati relativi a condanne e reati	1
Lavoro e sicurezza	1
Totale	28

Tabella 4. Tipologia delle decisioni su ricorsi

Decisioni su ricorsi	
Tipi di decisione (**)	Numero ricorsi
Accoglimento	15
Parziale accoglimento	8
Non luogo a provvedere (***)	74
Infondatezza	9
Inammissibilità	24
Totale (****)	130

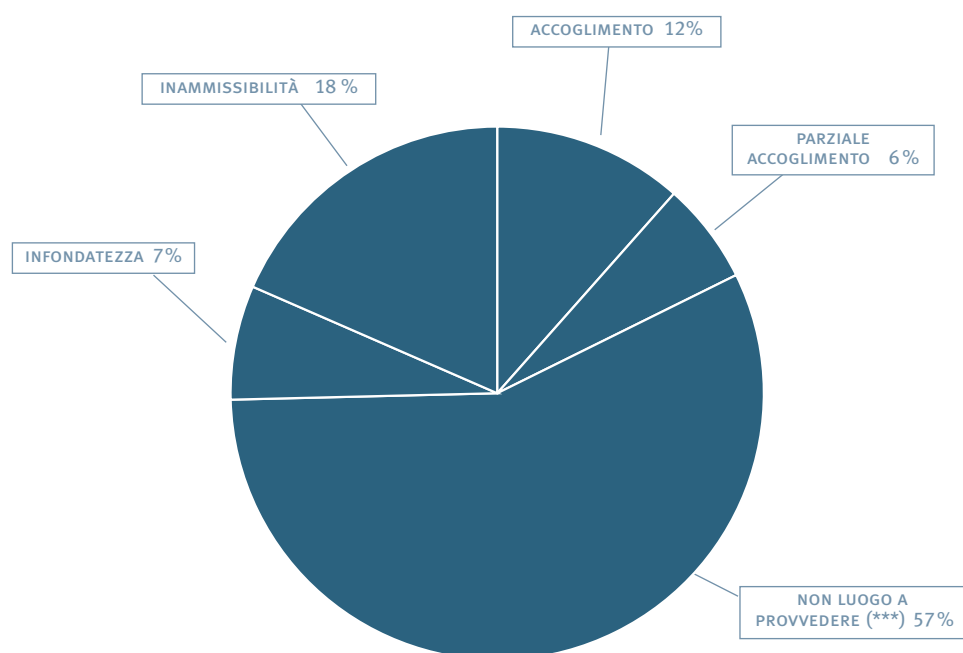
(*) Inerenti anche ad affari pervenuti anteriormente al 2018
(**) Le decisioni sui ricorsi possono contenere più statuizioni in base alle diverse richieste presentate: la statistica prende in esame, in tali casi, la statuizione più "favorevole" al ricorrente
(***) Casi nei quali le richieste del ricorrente sono state soddisfatte nel corso del procedimento
(****) Dati al 28 giugno 2018

Categorie di titolari	
	Numero ricorsi
Banche e società finanziarie	14
Compagnie di assicurazione	5
Sistemi di informazioni creditizie	3
Società di informazioni commerciali	7
Amministrazioni pubbliche e concessionari di pubblici servizi	8
Strutture sanitarie pubbliche e private	1
Fornitori telefonici e telematici	7
Attività di marketing svolta da imprenditori privati	5
Datori di lavoro pubblici e privati	11
Editori (anche televisivi)	51
Liberi professionisti	4
Amministrazioni condominiali	1
Associazioni	1
Altro	12
Totale (*)	130

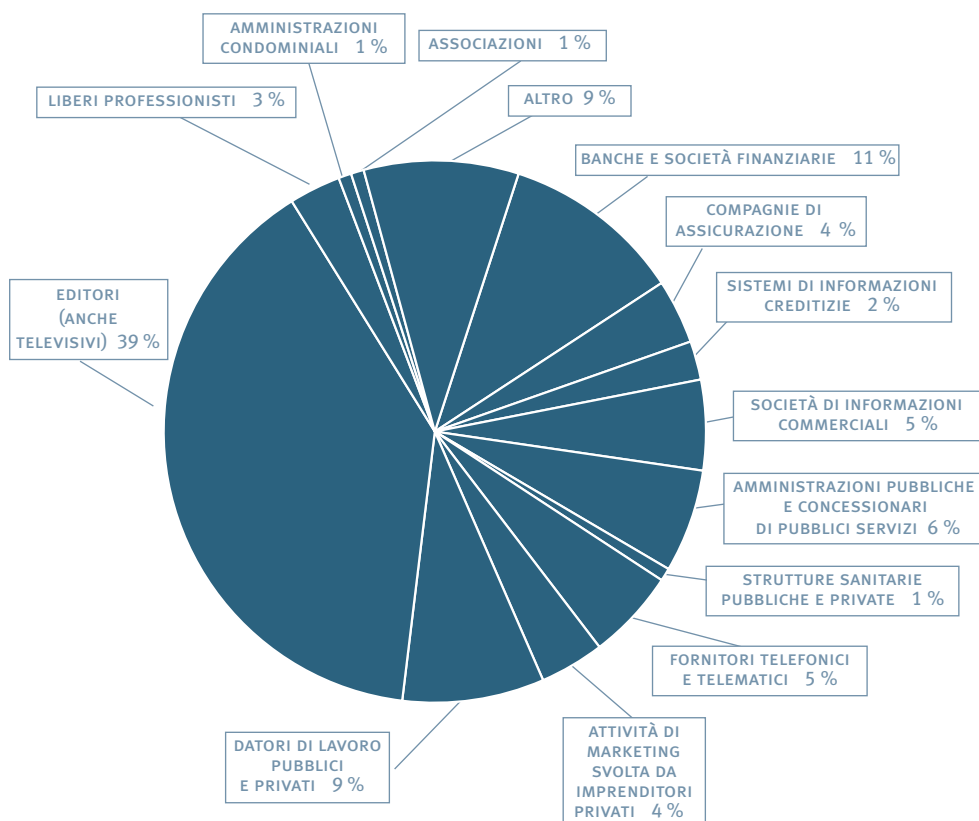
Tabella 5. Suddivisione dei ricorsi in relazione alle categorie di titolari del trattamento

(*) Dati al 28 giugno 2018

Tabella 6. Violazioni amministrative contestate

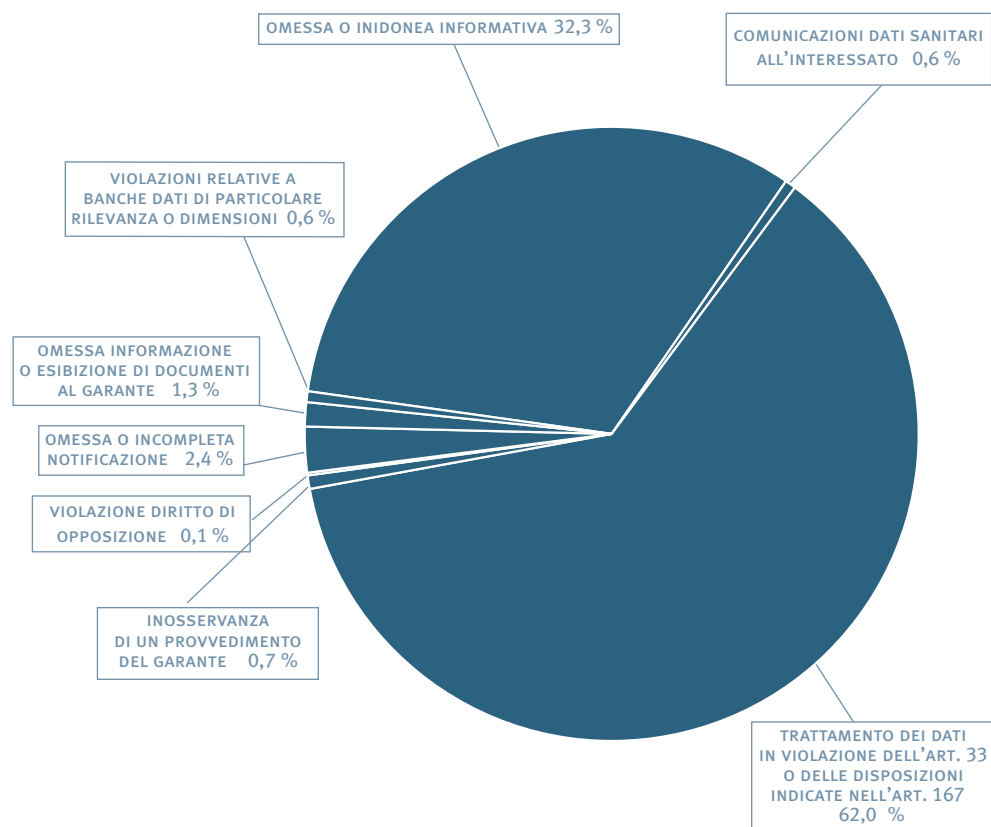
Violazioni amministrative contestate	
Omessa o inidonea informativa (art. 161, d.lgs. n. 196/2003)	229
Violazione delle modalità di comunicazione di dati sanitari all'interessato (art. 162, comma 2, d.lgs. n. 196/2003)	4
Trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis,* d.lgs. n. 196/2003)	438
Inosservanza di un provvedimento del Garante (art. 162, comma 2-*ter,* d.lgs. n. 196/2003)	5
Violazione del diritto di opposizione (art. 162, comma 2-*quater,* d.lgs. n. 196/2003)	1
Omessa o incompleta notificazione (art. 163, d.lgs. n. 196/2003)	17
Omessa informazione o esibizione di documenti al Garante (art. 164, d.lgs. n. 196/2003)	9
Violazioni relative a banche dati di particolare rilevanza o dimensioni (art. 164-*bis,* comma 2, d.lgs. n. 196/2003)	4
Totale	707

Comunicazioni di notizia di reato all'autorità giudiziaria	
	Segnalazioni
Trattamento illecito dei dati (art. 167, d.lgs. n. 196/2003)	1
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168, d.lgs. n. 196/2003)	1
Omessa adozione delle misure di sicurezza (art. 169, d.lgs. n. 196/2003)	14
Inosservanza di provvedimenti del Garante (art. 170, d.lgs. n. 196/2003)	2
Altre fattispecie (art. 171, d.lgs. n. 196/2003)	7
Violazioni di natura penale segnalate all'autorità giudiziaria	2
Totale	27

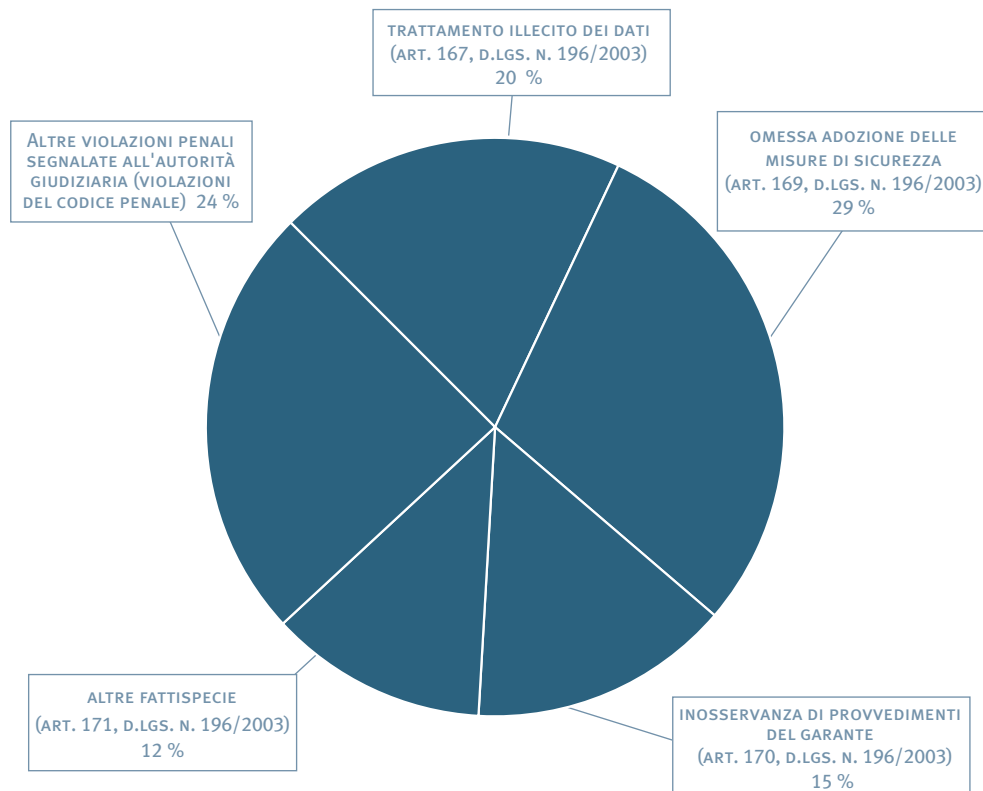
Tabella 7. Comunicazioni di notizia di reato all'autorità giudiziaria

Pagamenti derivanti dall'attività sanzionatoria	
Somme versate a titolo di oblazione in via breve	1.305.600
Somme versate in conseguenza di ordinanze ingiunzione	5.362.262
Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169, d.lgs. n. 196/2003)	90.000
Ulteriori entrate derivanti dall'attività sanzionatoria	1.017.544
Entrate dalla definizione agevolata dei procedimenti sanzionatori (art. 18, d.lgs. n. 101/2018)	386.400
Totale	**8.161.806**

Tabella 8. Pagamenti derivanti dall'attività sanzionatoria

Quesiti		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale quesiti	**769**	**310**

Tabella 9. Quesiti

(*) Inerenti anche ad affari pervenuti anteriormente al 2018

Tabella 10. Segnalazioni e reclami

Segnalazioni e reclami		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale segnalazioni e reclami	**7.458**	**5.330**
Temi principali		
Assicurazioni centrali	18	18
Assicurazioni	79	65
Associazioni	57	35
Centrali rischi	177	104
Concessionari pubblici servizi	120	83
Condominio	51	36
Credito	329	209
Enti locali	125	125
Imprese	305	177
Informazioni commerciali	20	5
Istruzione	76	76
Lavoro	263	166
Marketing (posta cartacea, e-mail, fax, sms)	1385	744
Marketing telefonico	1902	2178
Recupero crediti	131	51
Sanità e servizi di assistenza sociale	119	119
Trasparenza	64	64
Tributi	31	31
Videosorveglianza	300	201

Tabella 11. Tipologie di notificazioni pervenute: 2004-2018

Tipologie di notificazioni pervenute: 2004-2018 (**)			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute
Prima notificazione al Garante	1.403	24.336	25.739
Modifica di una precedente notificazione	231	5.508	5.739
Notificazione della cessazione del trattamento	126	1.413	1.539
Totale	**1.760**	**31.257**	**33.017**

(*) Inerenti anche ad affari pervenuti anteriormente al 2018
(**) I dati nella tabella sono riferiti alla data del 24 maggio 2018

Suddivisione delle notificazioni per tipologia di trattamento effettuato 2004-2018	
Tabelle di notificazione compilate (*)	Numero
Tabella 1 - Trattamento di dati genetici	3.372
Tabella 2 - Trattamento di dati biometrici	3.334
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	5.738
Tabella 4 - Trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria	9.072
Tabella 5 - Trattamento di dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale	918
Tabella 6 - Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con l'esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi	15.246
Tabella 7 - Trattamento di dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie	2.537
Tabella 8 - Trattamento di dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti	7.794
Totale (**)	**48.011**

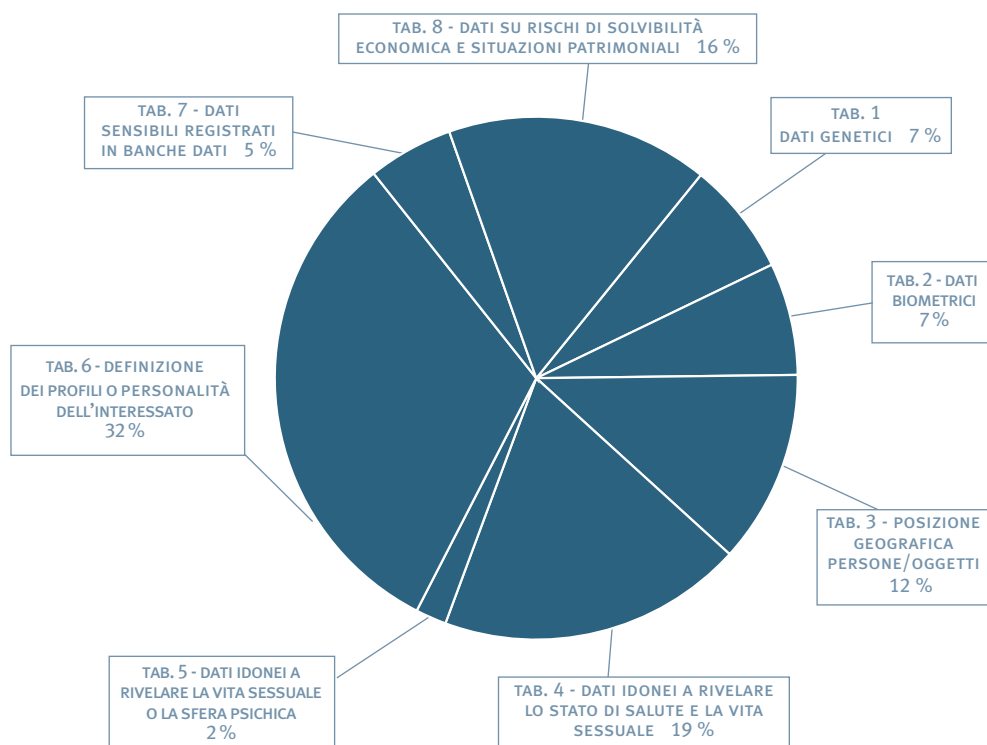
Tabella 12. Suddivisione delle notificazioni per tipologia di trattamento effettuato 2004-2018

(*) Situazione alla data del 24 maggio 2018
(**) N.B. Il totale è superiore a quello della precedente tabella in quanto una singola notificazione può riguardare più trattamenti

Tabella 13. Tipologie di notificazioni pervenute nel 2018

Tipologie di notificazioni pervenute nel 2018 (*)			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute
Prima notificazione al Garante	37	536	573
Modifica di una precedente notificazione	3	183	186
Notificazione della cessazione del trattamento	–	20	20
Totale	**40**	**739**	**779**

Tabella 14. Ufficio relazioni con il pubblico

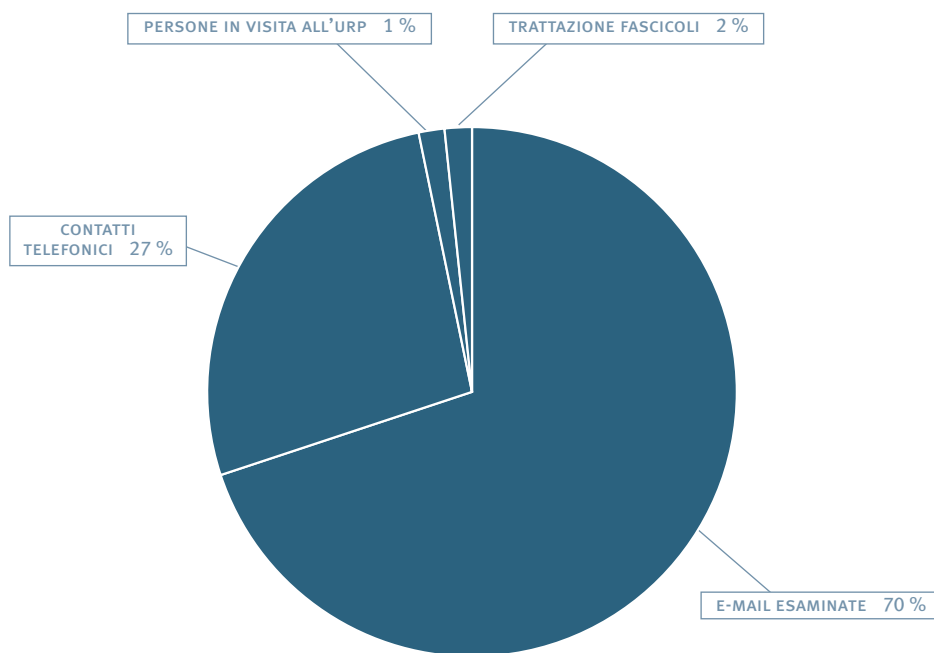
Ufficio relazioni con il pubblico	
	2018
E-mail esaminate	15.942
Contatti telefonici	6.122
Persone in visita all'Urp	359
Trattazione pratiche relative a fascicoli	379
Totale	**22.802**

(*) I dati nella tabella sono riferiti alla data del 24 maggio 2018

Grafico 15. E-mail esaminate dall'Ufficio relazioni con il pubblico

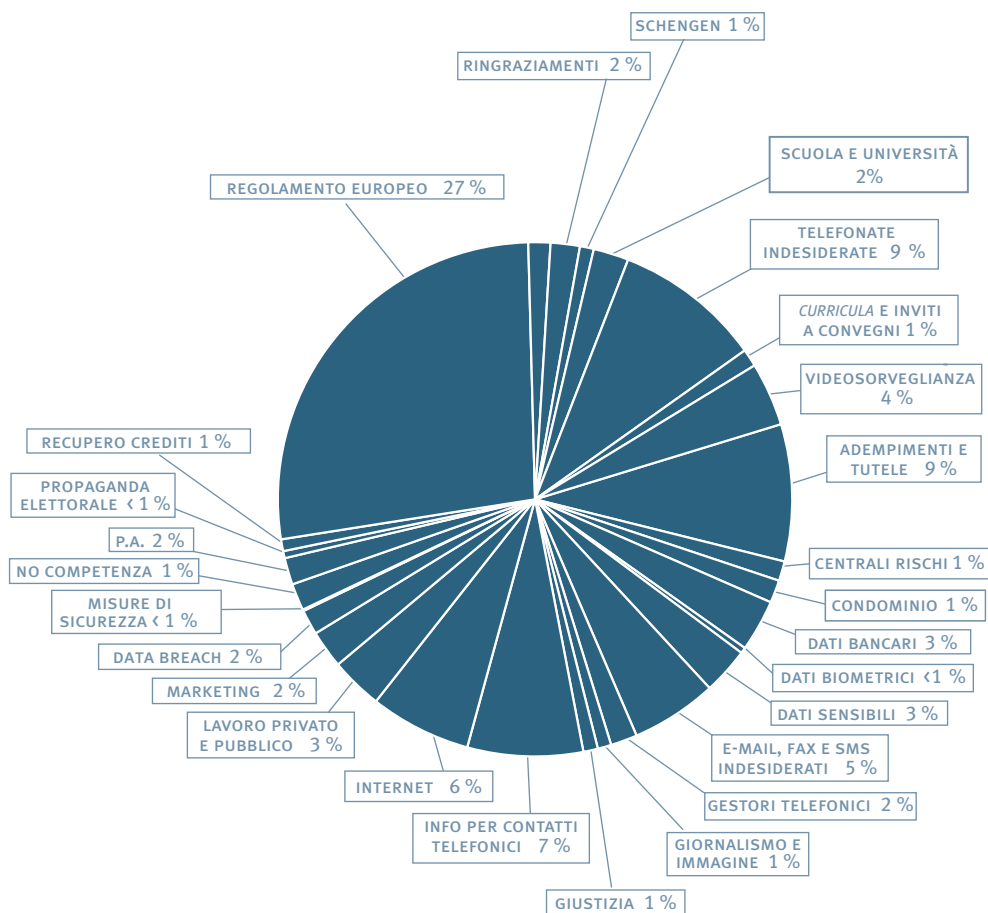
Tabella 16. Posti previsti in organico

Posti previsti in organico	
Segretario generale	1
Dirigenti	21
Funzionari	109
Operativi	29
Esecutivi	2
Totale	162
Personale a contratto	8

Tabella 17. Personale in servizio

Personale in servizio (*)				
Area	In ruolo (a)	In posizione di fuori ruolo (b)	Comandato presso altre amministrazioni o in aspettativa (c)	Impiegato dall'Ufficio (a+b-c)
Segretario generale	1	–	–	1
Dirigenti	13			13
Funzionari	82	4	2	84
Operativi	22			22
Esecutivi	–	–	–	–
Totali	**118**	**4**	**2**	**120**
Personale a contratto				5

Tabella 18. Risorse finanziarie

Risorse finanziarie				
Entrate accertate	**Anno 2018**	**Anno 2017**	**Variazione**	
Entrate correnti	26.927.498	21.061.842	5.865.656	27,85%
Totale entrate	**26.927.498**	**21.061.842**		**27,85%**
Spese impegnate	**Anno 2018**	**Anno 2017**	**Variazione**	
Spese di funzionamento	22.882.095	18.731.999	4.150.096	22,16%
Spese in c/capitale	212.363	259.305	-46.942	-18,10%
Trasferimenti ad amministrazioni	360.775	436.600	-75.825	-17,37%
Totale spese	**23.455.232**	**19.427.903**	**4.027.329**	**20,73%**

(*) Situazione alla data del 31 dicembre 2018

Tabella 19. Attività internazionali dell'Autorità

Unione europea			
Gruppo Articolo 29	Sessione plenaria Gruppo Art. 29		6-7 febbraio 10-11 aprile
	Comitato europeo per la protezione dati		24 -25 maggio 4-5 luglio 3 ottobre 16 novembre 3-4 dicembre
	Riunioni dei sottogruppi	*Border Travel Law Enforcement* (BTLE)	10 gennaio 15 marzo 26 aprile 26 giugno 30 ottobre 18 dicembre
		Cooperation	10 gennaio 7-8 marzo 15 maggio 13-14 novembre
		E-Government	25 gennaio 22 marzo 2 maggio 18 ottobre 13 dicembre
		Financial Matters	17 gennaio 20 marzo 18 aprile 15 novembre
		Future of Privacy	19 gennaio 20 marzo 14 maggio 19 giugno
		Key Provisions	18 gennaio 15 marzo 19 aprile 7 giugno 8 novembre
		International Transfers	8-9 gennaio 6-7 marzo 24 aprile 12-13 giugno 16-17 ottobre 12 novembre 11-12 dicembre
		Technology	16-17 gennaio 27 febbraio *(Google task force)* 20-21 marzo 23-24 aprile 14 giugno 6-7 novembre 19 dicembre

Gruppo Articolo 29	Riunioni dei sottogruppi	IMI-GDPR *Users Group*	8-9 febbraio 23 marzo 26-27 aprile 3-4 maggio 11 ottobre
		Enforcement	15 gennaio 8 marzo 8 maggio 12 novembre
		Fining Task Force	9 marzo 16 maggio 15 novembre
		Social Media Working Group	15 maggio 9 novembre
	Riunioni gruppi *ad hoc*	*Secondment Program Meeting*	24 settembre
		Coordinatori dei sottogruppi del CEPD	15 giugno 10 settembre

Unione europea	
Europol Cooperation Board	22-25 maggio (ispezione) 30 maggio 3 ottobre
Gruppo di coordinamento della supervisione SID	29 maggio 2 ottobre
Gruppo di coordinamento della supervisione SIS II	12-13 giugno 14 novembre
Gruppo di coordinamento della supervisione Eurodac	12-13 giugno 15 novembre
Gruppo di coordinamento della supervisione VIS	12-13 giugno 15 novembre

Unione europea	
Riunioni di gruppi di esperti	
ENISA *Expert Group* Art. 32 *GDPR*	8-9 ottobre
C- ITS *Intelligent Transport System WG*	29 marzo 30 maggio 18 dicembre
European Commission Workshop on GDPR (Privacy by Design)	1-2 febbraio, Praga
Second CPC Workshop with Data Protection Authorities	23 novembre, Bruxelles

Altri *forum* internazionali		
Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	Comitato WPSPDE *"Working Party on Security and Privacy in the Digital Economy"* - *Bureau* e Plenaria	13-14 novembre, Parigi
Consiglio d'Europa	Comitato Consultivo Convenzione 108/1981 (T-PD)	19-21 giugno, Strasburgo 20-22 novembre, Strasburgo
	T-PD *Bureau*	26-28 marzo, Parigi 17-19 dicembre, Strasburgo
Gruppi di lavoro specifici	Gruppo internazionale di lavoro sulla protezione dei dati nelle telecomunicazioni (IWGDPT)	9-10 aprile, Budapest 29-30 novembre, Queenstown

Conferenze internazionali	
Conferenza di primavera delle Autorità europee di protezione dati	3-4 maggio, Tirana
39ª Conferenza internazionale delle Autorità di protezione dati	22-26 ottobre, Bruxelles

Altre conferenze e *meeting*	
CPDP Conference	25 gennaio, Bruxelles
CEN-CENELEC *Technical Committee 8 "Privacy management in products and services"*	15 febbraio, Bruxelles 3 luglio, Berlino 14 dicembre, Delft
EU Project "Support to access to right on protection of Personal Data"	12-15 febbraio, Skopje
ETSI *Meeting on intelligent transport system*	7 marzo, Berlino
Incontro progetto UE "T4DATA"	13 marzo, Zagabria 8-11 ottobre, Varsavia
ISMS *Data Breach Forum*	8 marzo, Madrid
GDPR *Summit London Stock Exchange*	25 aprile, Londra
Incontro ISO/IEC 27552	4 luglio, Parigi
EU project DPEC- Big Data Health Sector	10-11 ottobre, Berlino
OECD *Expert Consultation, "Protecting Minors Online"*	15-16 ottobre, Zurigo
European Medicines Agency - Expert Group Anonymisation	23-24 ottobre, Londra
Incontro ISO/PC 317 *Consumer Protection – Privacy By Design for Consumer Goods and Services*	1-2 novembre, Londra
IX Conferenza internazionale *"Personal Data Protection"- Mosca*	8 novembre, Mosca
Convention 108 *Conference*	7-8 novembre, Città del Messico